ELSEVIER

Discrete Applied Mathematics 121 (2002) 193–202

DISCRETE APPLIED MATHEMATICS

On the bound for anonymous secret sharing schemes

Wataru Kishimoto[a], Koji Okada[b], Kaoru Kurosawa[b,*], Wakaha Ogata[c]

[a] *Department of Information and Image Sciences, Faculty of Engineering, Chiba University, 1-33 Yayoi-cho Inage-ku Chiba-shi, Chiba 263-8522, Japan*

[b] *Department of Communication and Integrated Systems, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan*

[c] *Center for Research in Advanced Financial Technology, Tokyo Institute of Technology, Tokyo, Japan*

Received 22 December 1999; received in revised form 6 November 2000; accepted 2 March 2001

Abstract

In anonymous secret sharing schemes, the secret can be reconstructed without knowledge of which participants hold which shares. In this paper, we derive a tighter lower bound on the size of the shares than the bound of Blundo and Stinson for anonymous (k,n)-threshold schemes with $1<k<n$. Our bound is tight for $k=2$. We also show a close relationship between optimum anonymous $(2,n)$-threshold secret schemes and combinatorial designs.

Keywords: Cryptography; Secret sharing scheme; Anonymous; Steiner system

1. Introduction

A (k,n)-threshold secret sharing scheme [1,7] is a method in which a dealer distributes a secret s to a set of n users in such a way that any k or more users can recover the secret s and any $k-1$ or less users have no information on s. On the other hand, in an anonymous secret sharing scheme, the secret can be reconstructed without knowledge of which participants hold which shares. In such schemes, the computation of the secret can be carried out by giving the shares to a black box that does not know the identities of the participants holding those shares. This would seem to be a desirable property in certain applications. For example, if the scheme is to be used to provide access to a secure area, then an anonymous scheme will provide security without the need for a separate identification protocol.

* Corresponding author. Department of Electrical and Electronic Engineering, Faculty of Engineering, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan.

E-mail addresses: kurosawa@titech.ac.jp (K. Kurosawa), wakaha@ss.titech.ac.jp (W. Ogata).

0166-218X/02/$ - see front matter
PII: S0166-218X(01)00236-0

Anonymous secret sharing schemes were first investigated by Stinson and Vanstone [8]. In the model proposed in [8], the participants receive distinct shares (we will call such a scheme a "strict" anonymous scheme). The authors proved a lower bound on the size of the shares and provided optimal schemes for certain class of threshold structures by using a combinatorial characterization of optimal schemes.

Next, Phillips and Phillips [6] considered a different model for anonymous secret sharing schemes. In their model, different participants are allowed to receive the same shares. They analyzed ideal anonymous secret sharing schemes in which the size of the shares given to each participant is equal to the size of the secret. The authors proved that an ideal anonymous (k,n)-threshold scheme can be realized if and only if $k=1$ or n.

Recently, Blundo and Stinson [2] showed a lower bound on the size of the shares for (k,n)-threshold schemes with $1<k<n$ together with another lower bound for an infinite class of access structures. They also presented constructions, some of which use Steiner systems.

In this paper, we derive a tighter lower bound on the size of the shares than the bound of Blundo and Stinson for anonymous (k,n)-threshold scheme with $1<k<n$. Our bound is tight for $k=2$. We also show a close relationship between optimum anonymous $(2,n)$-threshold secret schemes and resolvable Steiner systems.

2. Preliminaries

2.1. Notation and definitions

Let $\mathscr{P}=\{P_1,\ldots,P_n\}$ be a set of n participants and D be a dealer. Let S be a set of secrets and V be a set of shares. Suppose that the dealer D wants to share the secret $s\in S$ among the participants in $\mathscr{P}$.

We represent a secret sharing scheme by a collection of distribution rules. A *distribution rule* is a function

$$f:\mathscr{P}\cup\{D\}\to S\cup V$$

which satisfies the conditions $f(D)\in S$ and $f(P_i)\in V$ for $i=1,2,\ldots,n$. A distribution rule f represents a possible distribution of shares to participants, where $f(D)$ is the secret being shared, and $f(P_i)$ is the share given to P_i. If $s\in S$ is the secret that D wants to share, then D will choose a distribution rule f such that

$$f(D)=s$$

uniformly at random, and use f to distribute shares to participants.

Let $\{\Pr(s)\}_{s\in S}$ be a probability distribution on S. Let $\mathscr{F}$ be a family of distribution rules. We define (k,n)-threshold secret sharing schemes as follows.

Definition 2.1. A (k,n)-threshold secret sharing scheme is a collection of distribution rules $\mathscr{F}$ that satisfy the following two properties:

(1) If $A \subseteq \mathscr{P}$ and $|A| \geqslant k$, then for all $a = \{(P_i, v_i)\colon P_i \in A, v_i \in V\}$ with $\Pr(a) > 0$, a unique secret $s \in S$ exists such that $\Pr(s \mid a) = 1$.
(2) If $B \subseteq \mathscr{P}$ and $|B| \leqslant k-1$, then for all $b = \{(P_i, v_i)\colon P_i \in B, v_i \in V\}$ with $\Pr(b) > 0$, and for all secrets $s \in S$, it holds $\Pr(s \mid b) = \Pr(s)$.

Definition 2.2 (*Phillips and Phillips* [6] *and Blundo and Stinson* [2])**.** An *anonymous* (k,n)-threshold secret sharing scheme is a collection of distribution rules $\mathscr{F}$ which satisfies property (2) of Definition 2.1, as well as the following property:

(1′) If $A \subseteq \mathscr{P}$ and $|A| \geqslant k$, then for all $v = [v_i\colon P_i \in A, v_i \in V]$ with $\Pr(v) > 0$, a unique secret $s \in S$ exists such that $\Pr(s \mid v) = 1$.

Finally, we will use braces { } to denote sets and square brackets [ ] to denote multisets (a *multiset* is a set containing repeated elements).

2.2. Known results

Phillips and Phillips showed the following proposition [6].

Proposition 2.1. *There exists an anonymous* (k,n)*-threshold scheme such that* $|V| = |S|$ *if and only if* $k = 1$ *or* n.

Therefore, $|V| > |S|$ if $1 < k < n$ from [4,5]. Blundo and Stinson showed a lower bound on $|V|$ for $1 < k < n$ as follows [2].

Proposition 2.2. *In any anonymous* (k,n)*-threshold schemes with* $1 < k < n$,

$$|V| > \left[(n-k+2)\frac{|S|-1}{|S|} - 1\right](|S|-1).$$

3. Tighter lower bound on $|V|$

In this section, we derive a tighter lower bound on $|V|$ than Proposition 2.2 for anonymous (k,n)-threshold schemes. Let

$$S = \{1, 2, \ldots, |S|\}.$$

For each $f \in \mathscr{F}$, define

$$B_f \triangleq [f(P_j)\colon k-1 \leqslant j \leqslant n],$$

where B_f is a multiset. We call B_f a block.

Fix a distribution rule $f_0 \in \mathscr{F}$ arbitrarily and define

$$\mathscr{F}_i \triangleq \{f \in \mathscr{F}\colon f(D) = i, f(P_j) = f_0(P_j) \text{ for } 1 \leqslant j \leqslant k-2\},$$

$$\mathscr{A}_i \triangleq [B_f\colon f \in \mathscr{F}_i],$$

$$\mathscr{A}_0 \triangleq \mathscr{A}_1 \cup \mathscr{A}_2 \cup \cdots \cup \mathscr{A}_{|S|}.$$

Suppose that $x \in V$ occurs c_x^f times in B_f. Let

$$c_x^i \triangleq \sum_{f \in \mathscr{F}_i} c_x^f.$$

Then Blundo and Stinson showed the following proposition.

Proposition 3.1 (Blundo and Stinson [2, p. 20]). *In any anonymous (k,n)-threshold secret sharing scheme with $1 < k < n$:*

(1) *There exists a constant c_x such that*

$$c_x^i = c_x$$

for any $i \in S$.
(2) *If $[x, y]$ occurs in some block B_f such that $f(D) = i$, then $[x, y]$ occurs in no block $B_{f'}$ such that $f'(D) \neq i$.*

3.1. Our lower bound

Now we present our lower bound. Let

$$c \triangleq \max_{x \in V} c_x.$$

Theorem 3.1. *In any anonymous (k,n)-threshold secret sharing scheme with $1 < k < n$,*

$$|V| \geqslant (|S| - 1)(n - k + 1) + 1.$$

Proof. Choose $x_0 \in V$ such that

$$c_{x_0} = c$$

arbitrarily. Then there are two cases.

Case 1: $[x_0, x_0]$ appears in some block B_{f_1}. Suppose that $f_1(D) = s$. That is, $B_{f_1} \in \mathscr{A}_s$. From Proposition 3.1(2), $[x_0, x_0]$ appears in no block of any $\mathscr{A}_j$ with $j \neq s$. On the other hand, from Proposition 3.1(1), x_0 occurs in exactly c blocks of $\mathscr{A}_j$. Now for $j \neq s$, let

$$D_j \triangleq \{B_f | x_0 \in B_f, B_f \in A_j\}.$$

Then we have $|D_j| = c$. Define M_j be the $c \times (n-k+2)$ matrix such that each $B_f \in D_j$ is a row of M_j. Let

$$Y_j \triangleq \{y | y \in M_j, y \neq x_0\}.$$

Note that each $y \in Y_j$ appears in M_j at most c_y times, where $c_y \leqslant c$. Count the elements (other than x_0) of M_j in two ways. Then

$$c(n-k+1) \leqslant \sum_{y \in Y_j} c_y \leqslant \sum_{y \in Y_j} c = c|Y_j|. \tag{1}$$

Hence

$$|Y_j| \geqslant n-k+1. \tag{2}$$

Next for any $j_1 \neq j_2$,

$$Y_{j1} \cap Y_{j2} = \emptyset$$

from Proposition 3.1(2). Consequently,

$$|V| \geqslant |\{x_0\}| + \sum_{j \neq s} |Y_j| \tag{3}$$

$$\geqslant 1 + (|S|-1)(n-k+1). \tag{4}$$

Case 2: $[x_0, x_0]$ occurs in no blocks. Then similarly to Case 1, we have

$$|Y_j| \geqslant n-k+1$$

for any $j \in S$. Therefore,

$$\begin{aligned} |V| &\geqslant |\{x_0\}| + \sum_{j} |Y_j| \\ &\geqslant |S|(n-k+1)+1 \\ &> (|S|-1)(n-k+1)+1. \end{aligned}$$ □

It is easy to see that this bound is tighter than Proposition 2.2.

3.2. Generalization

A qualified subset of $\mathscr{P}$ which can recover the secret is called an *access set*, and the family of all access sets is called the *access structure*, denoted by Γ.

Definition 3.1 (*Phillips and Phillips* [6] *and Blundo and Stinson* [2])**.** An *anonymous* secret sharing scheme for Γ is a collection of distribution rules which satisfy the following two properties:

(1) If $A \in \Gamma$, then for all $v = [v_i\colon P_i \in A, v_i \in V]$ with $\Pr(v) > 0$, a unique secret $s \in S$ exists such that $\Pr(s \mid v) = 1$.
(2) If $B \notin \Gamma$, then for all $b = \{(P_i, v_i)\colon P_i \in B, v_i \in V\}$ with $\Pr(b) > 0$, and for all secrets $s \in S$, it holds $\Pr(s \mid b) = \Pr(s)$.

Blundo and Stinson showed the following lower bound on $|V|$ by generalizing the proof of Proposition 2.2.

Definition 3.2. We say that $B \subseteq \mathscr{P}$ is a semi-maximal nonaccess set if $B \cup \{P_i\} \notin \Gamma$ for all $P_i \in \mathscr{P} \setminus B$ and $B \cup \{P_i, P_j\} \in \Gamma$ for all $\{P_i, P_j\} \subseteq \mathscr{P} \setminus B$.

Proposition 3.2 (Blundo and Stinson [2])**.** *Suppose that there exists a semi-maximal nonaccess set $B \subseteq \mathscr{P}$ in an anonymous secret sharing scheme for Γ. Then*

$$|V| > \left[(n - |B|)\frac{|S| - 1}{|S|} - 1\right](|S| - 1).$$

Let $\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_2, P_4\}, \{P_1, P_2\}\}$ be the minimal qualified set of an access structure on the set of participants $\mathscr{P} = \{P_1, P_2, P_3, P_4\}$. In this case, we can take $B = \{P_3\}$.

Corollary 3.1 (Blundo and Stinson [2])**.** *In any anonymous secret sharing scheme for Γ_0,*

$$|V| > 2|S| - 5 + \frac{3}{|S|}.$$

On the other hand, by generalizing the proof of Theorem 3.1, we can obtain the following lower bounds.

Theorem 3.2. *Suppose that there exists a semi-maximal nonaccess set $B \subseteq \mathscr{P}$ in an anonymous secret sharing scheme for Γ. Then*

$$|V| \geqslant (n - |B| - 1)(|S| - 1) + 1.$$

Corollary 3.2. *In any anonymous secret sharing scheme for Γ_0,*

$$|V| \geqslant 2|S| - 1.$$

It is clear that our bounds are tighter than Proposition 3.2 and Corollary 3.1.

4. Relationship with combinatorial designs

4.1. Steiner systems

We now present some basic terminology from design theory. A k-(v, n, λ) design is a pair $(V, \mathscr{B})$, where V is a set of v elements and $\mathscr{B}$ is a family of subsets of V of size n (called blocks), such that every subset of elements of size k appears in exactly λ blocks. A k-(v, n, λ) design is said to be *nontrivial* if $k < n < v$. A *Steiner system* is a k-$(v, n, 1)$ design, also denoted by $S(k, n, v)$. Let $(V, \mathscr{B})$ be a Steiner system. We say that $(V, \mathscr{B})$ is partitionable if we can partition the set of blocks $\mathscr{B}$ into sets $\mathscr{B}_1, \ldots, \mathscr{B}_\ell$ in such a way that each $(V, \mathscr{B}_j)$, for $1 \leqslant j \leqslant \ell$, is a Steiner system $S(k-1, n, v)$. If a Steiner system is partitionable, then the integer $\ell = (v - k + 1)/(n - k + 1)$. A

partitionable $S(2,n,v)$ is called *resolvable*. For general information on the existence of k-(v,n,λ) designs, we refer to [3].

Blundo and Stinson showed the following proposition [2].

Proposition 4.1. *If there exists a resolvable Steiner system $S(2,n,|V|)$, then there exists an anonymous $(2,n)$-threshold scheme with $|V|=(|S|-1)(n-1)+1$.*

4.2. Relationship between optimum schemes and Steiner systems

We say that an anonymous (k,n)-threshold secret sharing scheme is optimum if the equality of Theorem 3.1 is satisfied. Then we obtain the following theorem immediately from Proposition 4.1.

Theorem 4.1. *There exists an optimum anonymous $(2,n)$-threshold secret sharing scheme if there exists a resolvable Steiner system $S(2,n,|V|)$.*

This theorem implies that Theorem 3.1 is tight for $k=2$.

We next prove a weak converse of Theorem 4.1. That is, we prove that there exists a Steiner system $S(2,n,|V|)$ (not necessarily resolvable) if there exists an optimum anonymous $(2,n)$-threshold secret sharing scheme.

In what follows, suppose that there exists an optimum anonymous (k,n)-threshold secret sharing scheme. Then the following lemmas hold from the proof of Theorem 3.1. (We use the same notation as in the proof of Theorem 3.1.)

Lemma 4.1. *Case 2 does not occur and all the equalities of Case 1 are satisfied.*

Proof. From the proof of Theorem 3.1. □

Lemma 4.2. *Each block $B_f=[b_{k-1},b_k,\ldots,b_n]\in\mathscr{A}_0$ must satisfy either*

$$b_{k-1}=b_k=\cdots=b_n$$

or

$$b_i\neq b_j \text{ for any } i\neq j.$$

Proof. Note that

$$c_x=c$$

for any $x\in V$ from the equality of Eq. (1). Therefore, the proof of Case 1 holds for any $x_0\in V$.

Suppose that some $[x_0,x_0]$ appears in $B_f\in\mathscr{A}_0$. Then from the equality of Eq. (4), we must have

$$B_f=[x_0,x_0,\ldots,x_0]. \qquad \square$$

Lemma 4.3. *If $B\in D_j$, then all the elements of B are distinct.*

Proof. From the definition of D_j, $[x_0, x_0]$ does not appear in any $B \in D_j$. Therefore, B contains $\{x_0, y\}$ such that $y \neq x_0$. Then form Lemma 4.2, all the elements of B are distinct. □

Now for each j with $j \neq s$, choose one block $\tilde{B}_j \in D_j$ arbitrarily. Let

$$\mathscr{B} \triangleq \{\tilde{B}_j | j \neq s\}.$$

We will prove that $(\mathscr{B}, V)$ is a Steiner system $S(2, n, |V|)$ for $k = 2$.

Lemma 4.4. *Any $B \in D_j$ is a permutation of $\tilde{B}_j$*

Proof. From Lemma 4.3 and the equality of Eq. (2). □

Lemma 4.5. *Any two distinct elements $\{x_0, y\}$ appear in at least one block of $\mathscr{B}$.*

Proof. From the equality of Eq. (3), any $\{x_0, y\}$ appears in some block $B' \in D_j$ with $j \neq s$.

On the other hand, from Lemma 4.4, any $B' \in D_j$ is a permutation of $\tilde{B}_j$. Therefore, $\{x_0, y\}$ is included in $\tilde{B}_j$. Hence, $\{x_0, y\}$ appears in some block of $\mathscr{B}$. □

Proof. Note that

$$|B_f| = n - k + 2 = n$$

if $k = 2$. First, suppose that some two distinct elements $\{x_0, y\}$ appear in two or more blocks of $\mathscr{B}$. These blocks must belong to the same $\mathscr{A}_h$ because $\{x_0, y\}$ determines the secret h uniquely ($k = 2$). However, we choose one block from $\mathscr{A}_h$ to construct $\mathscr{B}$. This is a contradiction.

Then from Lemma 4.5, any two distinct elements appear in exactly one block of $\mathscr{B}$. Therefore, $(\mathscr{B}, V)$ is a Steiner system $S(2, n, |V|)$. □

5. Impossibility for $k \geqslant 3$

In this section, we show that the equality of Theorem 3.1 cannot be satisfied for $3 \leqslant k < n$.

Definition 5.1. We say that $\{P_1, \cdots, P_{k-2}\}$ is a base set of the participants.

Theorem 5.1. *In any anonymous (k, n)-threshold secret sharing scheme with $3 \leqslant k < n$,*

$$|V| > (|S| - 1)(n - k + 1) + 1.$$

Proof. Suppose that there exists an anonymous (k, n)-threshold scheme for some $3 \leqslant k < n$.

P_1 is included in the base set (see Definition 5.1) since $k-2 \geqslant 1$. For f_0 in the definition of $\mathscr{F}_i$, let $y = f_0(P_1)$.

From Lemma 4.3 and Lemma 4.5, there exists a $B_{f_1} \in \mathscr{A}_0$ such that y appears in B_{f_1} and all the elements of B_{f_1} are distinct. Without loss of generality, we can suppose that $f_1(P_n) = y$. Then we have that

$$f_0(P_1) = f_1(P_1) = f_1(P_n) = y, \tag{6}$$

$$f_1(P_{n-1}) \neq f_1(P_n). \tag{7}$$

Next, let $\{P_2, \ldots, P_{k-1}\}$ be a base set of the participants and define

$$\mathscr{F}'_i \triangleq \{f \in \mathscr{F}\colon f(D) = i, f(P_j) = f_1(P_j) \text{ for } 2 \leqslant j \leqslant k-1\},$$

$$B'_f \triangleq [f(P_j)\colon j = 1, k, k+1, \ldots, n],$$

$$\mathscr{A}'_i \triangleq [B_f\colon f \in \mathscr{F}'_i],$$

$$\mathscr{A}'_0 \triangleq \mathscr{A}'_1 \cup \cdots \cup \mathscr{A}'_{|S|}.$$

Then $[y, y]$ appears in $B'_{f_1} \in \mathscr{A}'_0$ from Eq. (5). Therefore, from Lemma 4.2, it must be that

$$B'_{f_1} = [y, \ldots, y].$$

However, this contradicts Eq. (6). □

By generalizing the proof of Theorem 5.1, we can strengthen Theorem 3.2 as follows.

Theorem 5.2. *Suppose that there exist two semi-maximal nonaccess sets B_1 and B_2 such that $|B_1| = |B_2| = m$ and $|\mathscr{P} \setminus (B_1 \cup B_2)| \geqslant 2$ in an anonymous secret sharing scheme for Γ. Then*

$$|V| > (n-m-1)(|S|-1) + 1.$$

Let $\Gamma_1 = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_5\}, \{P_3, P_4\}, \{P_3, P_5\}, \{P_4, P_5\}\}$ be the minimal qualified set of an access structure on the set of participants $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$. In this case, we can take $B_1 = \{P_1\}$ and $B_2 = \{P_2\}$. Note that

$$|\mathscr{P} \setminus (B_1 \cup B_2)| = |\{P_3, P_4, P_5\}| \geqslant 2.$$

Corollary 5.1. *In any anonymous secret sharing scheme for Γ_1,*

$$|V| > 3|S| - 2.$$

References

[1] G.R. Blakley, Safeguarding cryptographic keys, Proceedings of the AFIPS 1979 National Computer Conference, vol. 48, 1979, pp. 313–317.

[2] C. Blundo, D.R. Stinson, Anonymous secret sharing schemes, Discrete Appl. Math. 77 (1997) 13–28.
[3] C.J. Colbourn, J.H. Dinitz (Eds.), CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[4] E.D. Karnin, J.W. Green, M.E. Hellman, On secret sharing systems, IEEE Trans. Inform. Theory IT-29 (1982) 35–41.
[5] K. Kurosawa, K. Okada, Combinatorial lower bounds for secret sharing schemes, Inform. Process. Lett. 60 (6) (1996) 301–304.
[6] S.J. Phillips, N.C. Phillips, Strongly ideal secret sharing schemes, J. Cryptology 5 (1992) 185–191.
[7] A. Shamir, How to share a secret, Comm. ACM 22 (11) (1979) 612–613.
[8] D.R. Stinson, S.A. Vanstone, A combinatorial approach to threshold schemes, SIAM J. Discrete Math. 1 (2) (1988) 230–236.