ELSEVIER

Discrete Applied Mathematics 77 (1997) 13–28

DISCRETE APPLIED MATHEMATICS

Anonymous secret sharing schemes

C. Blundo[a], D.R. Stinson[b,*]

[a] *Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy*

[b] *Department of Computer Science and Engineering, and Center for Communication and Information Science, University of Nebraska-Lincoln, Lincoln NE 68588, USA*

Received 4 April 1995; revised 6 February 1996

Abstract

In this paper we study anonymous secret sharing schemes. Informally, 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. Phillips and Phillips gave necessary and sufficient conditions for the existence of an anonymous secret sharing scheme where the size of the shares given to each participant is equal to the size of the secret. In this paper, we provide lower bounds on the size of the share sets in any (t, w) threshold scheme, and for an infinite class of non-threshold access structures. We also discuss constructions for anonymous secret sharing schemes, and apply them to access structures obtained from complete multipartite graphs.

1. Introduction

Informally, a secret sharing scheme is a method of distributing a secret key κ among a set of participants $\mathscr{P}$ in such a way that qualified subsets of $\mathscr{P}$ can reconstruct the value of κ, whereas any other (non-qualified) subsets of $\mathscr{P}$ cannot determine anything about the value of κ.

Secret sharing schemes are useful in any important action that requires the concurrence of several designated people to be initiated, such as launching a missile, opening a bank vault or even opening a safety deposit box. Secret sharing schemes are also used in management of cryptographic keys and multi-party secure protocols (see [12] for example).

The first secret sharing schemes that were studied are (t, w) threshold schemes. A (t, w) threshold scheme allows a secret to be shared among w participants in such a way that any t of them can recover the secret, but any $t-1$ have absolutely no information on the secret. Shamir [21] and Blakley [2] showed how to construct (t, w) threshold schemes. Subsequently, Ito et al. [14] and Benaloh and Leichter [1] described

* Corresponding author. E-mail: stinson@bibd.unl.edu.

PII S0166-218X(96)00101-1

a more general method of secret sharing. They showed how to realize a secret sharing scheme for any monotone access structure. (An *access structure* is the family of all subsets of participants that are able to reconstruct the secret).

The survey by Stinson [23] contains a unified description of results in the area of secret sharing schemes. For different approaches to the study of secret sharing schemes, including schemes with 'extended capabilities' such as disenrollment, fault-tolerance, and pre-positioning, and a complete bibliography, we recommend the survey article by Simmons [22].

An *ideal* secret sharing scheme is a scheme in which the size of the shares given to each participant is equal to the size of the secret. Brickell and Davenport [5] showed a correspondence between ideal secret sharing schemes and matroids (see also [15]).

In this paper we analyze anonymous secret sharing schemes. Informally, 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.

Anonymous secret sharing schemes were first investigated in 1988 by Stinson and Vanstone [26]. In the model proposed in [26] 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 for anonymous threshold schemes and provided optimal schemes for certain classes of threshold structures by using a combinatorial characterization of optimal schemes. Further results can be found in [20, 9].

In 1992, Phillips and Phillips [18] 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, referred to in [18] as 'strongly ideal schemes'. Phillips and Phillips proved the interesting result that a strongly ideal scheme for an access structure Γ on w participants can be realized if and only if Γ is either a $(1, w)$ threshold structure, a (w, w) threshold structure, or the closure of the edge set of a complete bipartite graph.

This paper is organized as follows: In Section 2 we give formal definitions for various types of secret sharing schemes, and introduce some notation used in the paper. In Section 3 we provide a lower bound on the size of the share set (as a function of the size of the key set) in any anonymous (t, w) threshold scheme, and for an infinite class of non-threshold access structures. In Section 4 we consider strict anonymous secret sharing schemes. We prove a lower bound on the size of the share set for non-threshold access structures, generalizing the bound proved in [26]. In Section 5 we present some constructions for anonymous secret sharing schemes. In particular, we look at access structures which are the closure of the edge set of a complete multipartite graph, that is, access structures for which the set of participants can be identified with the vertex set $V(G)$ of a graph $G = (V(G), E(G))$, and the subsets of participants qualified to

reconstruct the secret are only those containing an edge of G. (Non-anonymous secret sharing schemes for graph access structures have been extensively studied in several papers, such as [3–6, 8, 24, 25]).

2. Definitions and notation

A *perfect secret sharing scheme* permits a secret to be shared among a set $\mathscr{P}$ of w participants in such a way that a *qualified subset* of $\mathscr{P}$ can recover the secret, but any *non-qualified subset* has absolutely no information on the secret. An *access structure* Γ is the set of all subsets of $\mathscr{P}$ that can recover the secret.

Definition 2.1. Let $\mathscr{P}=\{P_1,\ldots,P_w\}$ be a set of participants. A *monotone access structure* Γ on $\mathscr{P}$ is a subset $\Gamma\subseteq 2^{\mathscr{P}}$, such that

$$A\in\Gamma,\quad A\subseteq A'\subseteq\mathscr{P}\Rightarrow A'\in\Gamma.$$

Definition 2.2. Let $\mathscr{P}=\{P_1,\ldots,P_w\}$ be a set of participants and let $A\subseteq 2^{\mathscr{P}}$. The *closure* of A, denoted $\mathsf{cl}(A)$, is the set

$$\mathsf{cl}(A)=\{C\colon \exists B\in A \text{ such that } B\subseteq C\subseteq\mathscr{P}\}.$$

For a monotone access structure Γ we have $\Gamma=\mathsf{cl}(\Gamma)$. If Γ is an access structure on $\mathscr{P}$, then $B\in\Gamma$ is a *minimal* qualified set if $A\notin\Gamma$ whenever $A\subseteq B$, $A\neq B$. The family of minimal qualified sets of Γ is denoted Γ_0 and is called the *basis* of Γ. We refer to a minimal qualified set as a *basis set*. It is easy to see that Γ is uniquely determined as a function of Γ_0, namely, $\Gamma=\mathsf{cl}(\Gamma_0)$. An access structure Γ will be called *trivial* if either $\Gamma=2^{\mathscr{P}}$ or $\Gamma=\{\mathscr{P}\}$ (i.e., if every set is a qualified set or if the only qualified set is the entire set of participants $\mathscr{P}$).

Let $\mathscr{K}$ be a set of q elements called *secrets* or *keys*, and let $\mathscr{S}$ be a finite set whose elements are called *shares*. Suppose a *dealer* D wants to share the secret key $\kappa\in\mathscr{K}$ among the participants in $\mathscr{P}$ (we will assume that $D\notin\mathscr{P}$). He does this by giving each participant $P\in\mathscr{P}$ a share from $\mathscr{S}$. The dealer can distribute the same shares to different participants, hence in the following we will use braces { } to denote sets and square brackets [ ] to denote multisets (a *multiset* is a set containing repeated elements).

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

$$f\colon\mathscr{P}\cup\{D\}\to\mathscr{K}\cup\mathscr{S}$$

which satisfies the conditions $f(D)\in\mathscr{K}$ and $f(P_i)\in\mathscr{S}$, for $i=1,2,\ldots,w$. A distribution rule f represents a possible distribution of shares to the participants, where $f(D)$ is the secret key being shared, and $f(P_i)$ is the share given to P_i. If $\mathscr{F}$ is a family of distribution rules and $\kappa\in\mathscr{K}$, then $\mathscr{F}_\kappa=\{f\in\mathscr{F}\colon f(D)=\kappa\}$ is the family of all distribution rules having κ as the secret. If $\kappa\in\mathscr{K}$ is the value of the secret that D

wants to share, then D will chose a distribution rule $f \in \mathscr{F}_\kappa$ uniformly at random, and use f to distribute shares to the participants.

Let $\{p_{\mathscr{K}}(\kappa)\}_{\kappa \in \mathscr{K}}$ be a probability distribution on $\mathscr{K}$, and let a collection of distribution rules for secrets in $\mathscr{K}$ be fixed. We define a perfect secret sharing scheme as follows.

Definition 2.3. A *perfect secret sharing scheme*, with respect to the monotone access structure $\Gamma \subseteq 2^{\mathscr{P}}$, is a collection of distribution rules that satisfy the following two properties:

1. If a subset $A \in \Gamma$ of participants pool their shares, then they can determine the value of the secret κ. *Formally, if* $A \in \Gamma$ *then for all* $a = \{(P_i, s_i)\colon P_i \in A \text{ and } s_i \in \mathscr{S}\}$ *with* $p(a) > 0$, *a unique secret* $\kappa \in \mathscr{K}$ *exists such that* $p(\kappa|a) = 1$.
2. If a subset $A \notin \Gamma$ of participants pool their shares, then they can determine nothing about the value of the secret κ (in an information-theoretic sense), even with infinite computational resources. *Formally, if* $A \notin \Gamma$ *then for all* $a = \{(P_i, s_i)\colon P_i \in A \text{ and } s_i \in \mathscr{S}\}$ *with* $p(a) > 0$, *and for all* $\kappa \in \mathscr{K}$, *it holds* $p(\kappa|a) = p_{\mathscr{K}}(\kappa)$.

Property 1 means that the values of the shares held by $A \in \Gamma$ and the identities of the participants in A completely determine the secret $\kappa \in \mathscr{K}$. Property 2 means that the probability that the secret is equal to κ, given that the shares held by $A \notin \Gamma$ and the identities of the participants in A are specified by a, is the same as the *a priori* probability of the secret κ. (From this it follows that for all $a = \{(P_i, s_i)\colon P_i \in A\}$, there exists an integer λ_a such that, for every $\kappa \in \mathscr{K}$, there exist exactly λ_a distribution rules $f \in \mathscr{F}_\kappa$ such that $f(P_i) = s_i$ for all $P_i \in A$.) Therefore, no amount of knowledge of shares of participants not qualified to reconstruct the secret enables a Bayesian opponent to modify an a priori guess regarding the secret.

Throughout this paper, we confine our attention to perfect schemes, so the term 'secret sharing scheme' can be taken to mean 'perfect secret sharing scheme'.

A secret sharing scheme for which $|\mathscr{K}| = |\mathscr{S}|$ is called an *ideal* secret sharing scheme and an access structure admitting an ideal scheme will be referred as *ideal access structure*.

We assume that the secret reconstruction phase is carried out by a trustworthy machine that keeps secret all the received shares. This is not a strong assumption and it is more or less explicitly used in all usual secret sharing schemes. In fact, if the machine does not keep the received shares secret, then everyone who has access to the machine would know all the shares and therefore could reconstruct the secret even if he is not allowed to.

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 trustworthy machine that does not know the identities of the participants holding those shares. The difference between a secret sharing scheme and an anonymous secret sharing scheme depends on the reconstruction function used by the trustworthy machine.

We define an anonymous secret sharing scheme as follows.

Definition 2.4. An *anonymous secret sharing scheme*, with respect to the monotone access structure $\Gamma \subseteq 2^{\mathscr{P}}$, is a collection of distribution rules which satisfies Property 2 of Definition 2.3, as well as the following property:

1. If a subset $A \in \Gamma$ of participants pool their shares (but keep their identities secret), then they can determine the value of the secret κ. *Formally, if* $A \in \Gamma$ *then for all* $s = [s_i: P_i \in A \text{ and } s_i \in \mathscr{S}]$ *with* $p(s) > 0$, *a unique secret* $\kappa \in \mathscr{K}$ *exists such that* $p(\kappa|s) = 1$.

In this definition, Property 1 means that to compute the secret it is enough to know just the shares held by participants in a qualified set – it is not necessary to know the qualified set or which participants hold which shares.

Note that instead we could have used the following weaker security condition in the definition of an anonymous scheme:

2′. If a subset $A \notin \Gamma$ of participants pool their shares (but keep their identities secret), then they can determine nothing about the value of the secret κ (in an information-theoretic sense), even with infinite computational resources. *Formally, if* $A \notin \Gamma$ *then for all* $s = [s_i: P_i \in A \text{ and } s_i \in \mathscr{S}]$ *with* $p(s) > 0$, *and for all* $\kappa \in \mathscr{K}$, *it holds* $p(\kappa|s) = p_{\kappa}(\kappa)$.

However, in this paper, we will restrict our attention to schemes that satisfy Property 2 since most known constructions produce schemes that satisfy this 'stronger' condition. Moreover, it is generally better to use the strongest security condition in designing any cryptographic protocol.

Stinson and Vanstone [26] considered a model of anonymous secret sharing in which the participants receive distinct shares. We will refer to this model as a *strict* anonymous secret sharing scheme. A strict anonymous scheme can be considered as an anonymous scheme with an additional property.

We define a strict anonymous secret sharing scheme as follows.

Definition 2.5. A *strict anonymous secret sharing scheme*, with respect to the monotone access structure $\Gamma \subseteq 2^{\mathscr{P}}$, is a collection of distribution rules which satisfies Properties 1 and 2 of Definition 2.4, as well as the following property:

3. For any given secret key $\kappa \in \mathscr{K}$, the participants in $\mathscr{P}$ receive distinct shares. *Formally, for all* $\kappa \in \mathscr{K}$, *for all* $s \in \mathscr{S}$ *and for all* $P_i, P_j \in \mathscr{P}$, *it holds* $p(P_i = s,\ P_j = s|\kappa) = 0$.

The following example illustrates the three different models of secret sharing for a particular access structure.

Example 2.1. Let $\Gamma_0 = \{\{P_1P_2\}, \{P_1P_3\}, \{P_2P_3\}\}$ be the basis of a $(2,3)$ threshold structure, Γ, on the set of participants $\mathscr{P} = \{P_1, P_2, P_3\}$. We construct schemes for this access structure, in which the set $\mathscr{S}$ contains nine elements, for all three models.

An ideal scheme

We can realize an ideal secret sharing scheme (i.e. one in which there are nine possible keys) for Γ by using the technique of Shamir [21]. Let $\mathscr{S}=\mathscr{K}=GF(9)$. For any secret key $\kappa\in\mathscr{K}$ the family $\mathscr{F}_\kappa$ of distribution rules will be constructed as

$$\mathscr{F}_\kappa=\{(f_a(1),f_a(2),f_a(3)):\ f_a(x)=\kappa+ax,\ a\in GF(9)\}.$$

It is easy to see that the distribution rules thus obtained constitute an ideal secret sharing scheme for Γ. There are 81 distribution rules, nine for each possible secret key.

An anonymous scheme

The following collection of distribution rules comprise an anonymous scheme for Γ, in which there are five possible keys. (This scheme is an application of a construction given in Section 5.)

$$\begin{aligned}
\mathscr{F}_0&=\{(0,0,0),(1,1,1),(2,2,2),(3,3,3),(4,4,4),(5,5,5),(6,6,6),(7,7,7),\\
&\quad (8,8,8)\}\\
\mathscr{F}_1&=\{(0,1,2),(1,2,0),(2,0,1),(3,4,5),(4,5,3),(5,3,4),(6,7,8),(7,8,6),\\
&\quad (8,6,7)\}\\
\mathscr{F}_2&=\{(0,3,6),(3,6,0),(6,0,3),(1,4,7),(4,7,1),(7,1,4),(2,5,8),(5,8,2),\\
&\quad (8,2,5)\}\\
\mathscr{F}_3&=\{(0,4,8),(4,8,0),(8,0,4),(1,5,6),(5,6,1),(6,1,5),(2,3,7),(3,7,2),\\
&\quad (7,2,3)\}\\
\mathscr{F}_4&=\{(0,5,7),(5,7,0),(7,0,5),(1,3,8),(3,8,1),(8,1,3),(2,4,6),(4,6,2),\\
&\quad (6,2,4)\}
\end{aligned}$$

It is easy to check that we have an anonymous scheme for Γ. Indeed, each pair of shares $(x,y)\in(\mathbb{Z}_9\times\mathbb{Z}_9)$ belongs to only one $\mathscr{F}_\kappa$; hence the secret key is uniquely determined from any two shares. In each $\mathscr{F}_\kappa$, each possible share is assigned to each possible participant by exactly one distribution rule. Hence the secret key remains completely unknown, given a single share and the identity of the participant holding it. There are 45 distribution rules, nine for each possible secret key.

A strict anonymous scheme

The distribution rules in $\mathscr{F}_1,\mathscr{F}_2,\mathscr{F}_3$, and $\mathscr{F}_4$ comprise a strict anonymous scheme for Γ_0 in which there are four possible keys. (This scheme is an application of a construction given in [26], and is optimal with respect to the size of the share set.)

It is easy to check that these families of distribution rules realize an anonymous secret sharing scheme for Γ. Indeed, each pair of (distinct) shares $x,y\in\mathbb{Z}_9$ belongs to only one $\mathscr{F}_\kappa$, hence the secret key is uniquely determined; but any single share is assigned to any particular participant by exactly one distribution rule in each $\mathscr{F}_\kappa$, so the secret key remains completely unknown. There are 36 distribution rules, nine for each possible secret key.

2.1. Terminology from graph theory and design theory

We first present some basic terminology from graph theory. We consider only undirected graphs that do not have loops or multiple edges. If G is a graph, we denote the vertex set of G by $V(G)$ and the edge set by $E(G)$. In an undirected graph the pair of vertices representing any edge is unordered. Thus, the pairs (u,v) and (v,u) represent the same edge. A graph G is *connected* if any two vertices are joined by a path. The *complete graph* K_n is the graph on n vertices in which any two vertices are joined by an edge. The *complete multipartite graph* $K_{n_1,n_2,\ldots,n_t}$ is a graph on $\sum_{i=1}^{t} n_i$ vertices, in which the vertex set is partitioned into subsets of size n_i $(1 \leqslant i \leqslant t)$ called *parts*, such that (v,w) is an edge if and only if v and w are in different parts. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques. Note that the complete graph K_n can be thought of as a complete multipartite graph with n parts of size 1. A *stable set* or *independent set* of G is a subset of vertices $A \subseteq V(G)$ such that no two vertices in A are joined by an edge in $E(G)$. The *stability number* or *independence number* $\alpha(G)$ is defined to be the maximum cardinality of a stable set of G. A *dominating set* of a graph G is a set $V' \subseteq V(G)$ such that every vertex $v \in V(G) \backslash V'$ is joined to at least one element of V' by an edge in $E(G)$.

Given a graph G, we can obtain an access structure Γ based on G by computing the closure of the edge set $E(G)$. Each edge in the graph determines two participants who can recover the secret. In this situation, we will identify Γ_0 with the graph G.

We now present some basic terminology from design theory. A t-(v,k,λ) design is a pair $(V,\mathscr{B})$, where V is a set of v elements (called *points*) and $\mathscr{B}$ is a family of subsets of V of size k (called *blocks*), such that every subset of points of size t occurs in exactly λ blocks. A t-(v,k,λ) design is said to be *non-trivial* if $t < k < v$. A *Steiner system* is a t-$(v,k,1)$ design, also denoted by $S(t,k,v)$. Let $(V,\mathscr{B})$ be a Steiner system $S(t,k,v)$. 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 $S(t-1,k,v)$. If a Steiner system $S(t,k,v)$ is partitionable, then the integer $\ell = (v-t+1)/(k-t+1)$. A partitionable $S(2,k,v)$ is called *resolvable*. For general information on the existence of t-(v,k,λ) designs we refer to [10].

The following result will be used in the construction of anonymous secret sharing schemes for complete multipartite graphs.

Theorem 2.1. *For $2 \leqslant k \leqslant 4$, there exists a resolvable $S(2,k,v)$ if and only if $v \equiv k \bmod k(k-1)$.*

Proof. The case $k=2$ is trivial. In fact, a resolvable $S(2,2,v)$ is a one-factorization of K_v, the complete graph on v vertices. The proof of Theorem 2.1 for the case $k=3$ can be found in [19] (this is the well known 'Kirkman's schoolgirl problem'); for $k=4$, see [13]. □

Results on resolvable $S(2,k,v)$ for larger k can be found in [10].

3. Bounds on the size of the shares

The following theorem of Phillips and Phillips gives necessary and sufficient conditions for an ideal anonymous secret sharing scheme to exist.

Theorem 3.1 (Phillips and Phillips [18]). *Let Γ be an access structure on a set of participants $\mathscr{P}$. An ideal anonymous secret sharing scheme for Γ exists if and only if either Γ is a $(1,|\mathscr{P}|)$ threshold structure, a $(|\mathscr{P}|,|\mathscr{P}|)$ threshold structure, or the closure of a complete bipartite graph.*

In the remainder of this section, we provide lower bounds on the size of the share set as a function of the size of the key set in any (t,w) threshold scheme $(1<t<w)$, and for an infinite class of non-threshold access structures. From Theorem 3.1, we know that $|\mathscr{S}|>|\mathscr{K}|$, but the bound we prove in this section is an asymptotic improvement.

Theorem 3.2. *Let Γ be a (t,w) threshold structure with $1<t<w$. In any anonymous secret sharing scheme for Γ, with secrets in $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}|>\left[(w-t+2)\frac{|\mathscr{K}|-1}{|\mathscr{K}|}-1\right](|\mathscr{K}|-1).$$

Proof. Suppose the set of participants is $\mathscr{P}=\{P_i\colon 1\leqslant i\leqslant w\}$. Let $|\mathscr{S}|=v$, let $\mathscr{K}=\{1,\ldots,q\}$, and let $\mathscr{F}$ denote the collection of distribution rules of the scheme. Denote $h=w-t+2$. Choose any distribution rule $f_0\in\mathscr{F}$, and define

$$\mathscr{F}_0=\{f\in\mathscr{F}\colon f(P_i)=f_0(P_i),\ 1\leqslant i\leqslant t-2\}.$$

For any $f\in\mathscr{F}_0$, define

$$A_f=[f(P_i)\colon t-1\leqslant i\leqslant w].$$

(That is, we look at all the distribution rules that contain a fixed list of shares for a specified non-qualified set of participants, as was done in [16].) In this way we get a collection $\mathscr{A}=[A_f\colon f\in\mathscr{F}_0]$ of h–multisets of $\mathscr{S}$, which we refer to as *blocks*. Partition this collection of blocks into q subcollections, $\mathscr{A}_1,\ldots,\mathscr{A}_q$, determined by the corresponding keys for the distribution rules. This collection satisfies the following properties:

1. If x occurs c_x times in blocks in $\mathscr{A}_i$ (counting multiplicities), then x occurs exactly c_x times in blocks in $\mathscr{A}_j$, for $1\leqslant j\leqslant q$. (This follows from h applications of Property 2 of Definition 2.4, by taking A to be the h different subsets $A_j=\{P_1,\ldots,P_{t-2},P_j\}$, $t-1\leqslant j\leqslant w$.)

2. If $[x,y]$ occurs in a block in $\mathscr{A}_i$, then $[x,y]$ occurs in no blocks in $\mathscr{A}_j$ if $i\neq j$. (This follows from Property 1 of Definition 2.4.)

We observe that Property 1 implies that

$$|\mathscr{A}_i| = \frac{\sum_{x \in \mathscr{S}} c_x}{h}$$

for $1 \leqslant i \leqslant q$. We will denote this value by m.

Now for each block $A \in \mathscr{A}$, define $\tilde{A}$ to be the set consisting of the distinct points in A (i.e., the 'underlying set' of points in A). Let $\tilde{\mathscr{A}}_i = \{\tilde{A} : A \in \mathscr{A}_i\}$. Consider the incidence structure $\tilde{\mathscr{A}} = \{\tilde{\mathscr{A}}_1, \ldots, \tilde{\mathscr{A}}_q\}$. Any point x occurs at least $(q-1)c_x + 1$ times in $\tilde{\mathscr{A}}$, since the pair $[x,x]$ occurs in a block $A \in \mathscr{A}_i$ for at most one value of i.

The average block size δ in $\tilde{\mathscr{A}}$ satisfies the following inequality:

$$\delta \geqslant \sum_{x \in \mathscr{S}} \frac{(q-1)c_x + 1}{mq} > \frac{mh(q-1)}{mq} = \frac{h(q-1)}{q}. \tag{1}$$

Denote by $\alpha_i(x)$ the average size of the blocks in $\tilde{\mathscr{A}}_i$ containing x, and define

$$\alpha(x) = \sum_{i=1}^{q} \alpha_i(x).$$

Now, we have

$$\sum_{\{\tilde{A}: x \in \tilde{A}\}} |\tilde{A}| \leqslant c_x \sum_{i=1}^{q} \alpha_i(x) = c_x \alpha(x).$$

Then, we obtain the following:

$$\begin{aligned}
\sum_{x \in \mathscr{S}} c_x \alpha(x) &\geqslant \sum_{x \in \mathscr{S}} \sum_{\{\tilde{A}: x \in \tilde{A}\}} |\tilde{A}| = \sum_{A \in \mathscr{A}} |\tilde{A}|^2 \\
&\geqslant |\mathscr{A}| \left(\frac{\sum_{A \in \mathscr{A}} |\tilde{A}|}{|\mathscr{A}|} \right)^2 \quad \text{(from Jensen's inequality)} \\
&- mq\delta^2 \\
&> mq \left(\frac{h(q-1)}{q} \right)^2 \quad \text{(from (1))} \\
&= \frac{mh^2(q-1)^2}{q}.
\end{aligned}$$

Let $\alpha = \max\{\alpha(x): x \in \mathscr{S}\}$. Then, we have that

$$\sum_{x \in \mathscr{S}} c_x \alpha(x) \leqslant \sum_{x \in \mathscr{S}} c_x \alpha = \alpha \sum_{x \in \mathscr{S}} c_x = \alpha mh.$$

Hence we have that

$$\alpha > \frac{h(q-1)^2}{q}.$$

Consequently, there is a point $x \in \mathscr{S}$ such that

$$\alpha(x) > \frac{h(q-1)^2}{q}.$$

Consider $L = |\{y \neq x: \{x, y\} \subseteq \tilde{A} \text{ for some } \tilde{A}\}|$. Then, $L \leqslant v - 1$. But

$$\begin{aligned} L &\geqslant \sum_{i=1}^{q} (\alpha_i(x) - 1) \quad \text{(from property 2.)} \\ &= \alpha(x) - q > \frac{h(q-1)^2}{q} - q. \end{aligned}$$

Thus,

$$\begin{aligned} v &> \frac{h(q-1)^2}{q} - q + 1 \\ &= (w - t + 2)\frac{(q-1)^2}{q} - (q-1) \\ &= \left[(w - t + 2)\frac{(q-1)}{q} - 1\right](q-1), \end{aligned}$$

and the theorem is proved. □

The bound of the previous theorem is non-trivial (i.e., we get $|\mathscr{S}| > |\mathscr{K}|$) when $|\mathscr{K}| \geqslant 5$. The following theorem gives a lower bound on the size of the shares held by participants for an infinite class of non-threshold access structures.

Theorem 3.3. *Let Γ be an access structure on a set $\mathscr{P}$ of w participants. Suppose there exists a set $B \subseteq \mathscr{P}$ such that $B \cup \{P_i\} \notin \Gamma$ for all $P_i \in \mathscr{P} \backslash B$, and $B \cup \{P_i, P_j\} \in \Gamma$ for all $\{P_i, P_j\} \subseteq \mathscr{P} \backslash B$. Then, in any anonymous secret sharing scheme for Γ, with key set $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| > \left[(w - |B|)\frac{|\mathscr{K}| - 1}{|\mathscr{K}|} - 1\right](|\mathscr{K}| - 1).$$

Proof. Let $\mathscr{F}$ denote the collection of distribution rules of the scheme. Choose any distribution rule $f_0 \in \mathscr{F}$, and define

$$\mathscr{F}_0 = \{f \in \mathscr{F}: f(P_i) = f_0(P_i) \text{ for all } P_i \in B\}.$$

For any $f \in \mathscr{F}_0$, define

$$A_f = [f(P_i): P_i \in \mathscr{P} \backslash B].$$

Now repeat the remainder of the proof of Theorem 3.2, mutatis mutandis. □

As an example, consider the access structure having basis

$$\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_2, P_4\}, \{P_1, P_2\}\}.$$

In this case we can take $B = \{P_3\}$ and the following corollary holds.

Corollary 3.4. *Let $\Gamma_0 = \{\{P_1, P_3, P_4\}, \{P_2, P_4\}, \{P_1, P_2\}\}$ be the basis of an access structure on the set of participants $\mathscr{P} = \{P_1, P_2, P_3, P_4\}$. In any anonymous secret sharing scheme for Γ with a key set of size q, the size of the share set $\mathscr{S}$ satisfies*

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

4. Strict anonymous schemes

In this section we consider a different model of anonymous secret sharing scheme, where we require that the participants receive distinct shares. We will refer to such a scheme as a *strict* anonymous secret sharing scheme. This model was first investigated by Stinson and Vanstone [26] in the case of threshold schemes. Further results can be found in [20, 9].

Remark 4.1. Stinson and Vanstone investigated a slightly more restricted model in which a (t, w) threshold scheme is constructed from a w-uniform hypergraph. This involves defining $w!$ distribution rules from each hyperedge by ordering it in all possible ways. However, all results proved in [26] remain true in the more general model we consider in this paper.

Stinson and Vanstone [26] proved the following result.

Theorem 4.1 (Stinson and Vanstone [26]). *In any strict anonymous (t, w) threshold scheme, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| \geqslant (w - t + 1)|\mathscr{K}| + t - 1.$$

For an information-theoretic proof, see [7].

Here, we prove a lower bound on the size of the share set for general access structures, which contains the previous bound as a special case.

Theorem 4.2. *Let Γ be an access structure on a set $\mathscr{P}$ of w participants. Suppose that there exists a set $B \subseteq \mathscr{P}$ such that $|B| = r$, $B \notin \Gamma$, and $B \cup \{P_i\} \in \Gamma$ for all $P_i \in \mathscr{P} \backslash B$. Then, in any strict anonymous secret sharing scheme for Γ with key set $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| \geqslant (w - r)|\mathscr{K}| + r.$$

Proof. Let $\mathscr{F}$ denote the collection of distribution rules of the scheme. Choose any distribution rule $f_0 \in \mathscr{F}$, and define

$$\mathscr{F}_0 = \{f \in \mathscr{F} : f(P_i) = f_0(P_i) \text{ for all } P_i \in B\}.$$

For any $f \in \mathscr{F}_0$, define

$$A_f = [f(P_i) : P_i \in \mathscr{P} \backslash B].$$

In this way we get a collection $\mathscr{A} = [A_f : f \in \mathscr{F}_0]$ of $(w-r)$-multisets of $\mathscr{S}$, which we refer to as *blocks*. Partition this collection of blocks into q subcollections, $\mathscr{A}_1, \ldots, \mathscr{A}_q$, determined by the corresponding keys for the distribution rules.

Now, choose one set in each of these subcollections, say $A_i \in \mathscr{A}_i$ for $i = 1, 2, \ldots, q$. Since the scheme for Γ is a strict anonymous scheme, it is easy to see that the A_i's satisfy the following properties.

1. For $i = 1, 2, \ldots, q$, we have $S \cap A_i = \emptyset$.
2. For $i \neq j$, we have $A_i \cap A_j = \emptyset$ (for, if $x \in A_i \cap A_j$, then there correspond two different keys to the same set of shares, $S \cup \{x\}$, distributed to some qualified subset).

Hence, to construct a scheme for Γ, we need a share set of size at least $(w-r)|\mathscr{K}| + r$. □

Even though the conditions of Theorem 4.2 seem quite strict, for any access structure Γ there does exist a set B of participants satisfying them. In fact, it is sufficient to take the set B as a non-qualified set of maximum size. For threshold access structures, this yields the bound of Theorem 4.1. In the case of a graph access structure, the following corollary is obtained.

Corollary 4.3. *Let G be a graph on w vertices. Then, in any strict anonymous secret sharing scheme for G, with key set $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| \geq (w - \alpha(G))|\mathscr{K}| + \alpha(G),$$

where $\alpha(G)$ is the stability number of G.

In general, given a graph G, we want to find a set B satisfying the conditions of Theorem 4.2 such that the bound is maximized. Hence, the size of such a set B should be minimized. The best choice for B is to take a minimum size-independent set of G that is also a dominating set. We obtain the following.

Corollary 4.4. *Let G be a graph on w vertices. Then, in any strict anonymous secret sharing scheme for G with key set $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| \geq (w - \beta(G))|\mathscr{K}| + \beta(G),$$

where $\beta(G)$ is the minimum size of an independent set of G that is also a dominating set.

For general graphs, to compute the minimum size independent set that is also a dominating set is hard. Indeed, given an integer ℓ and a graph G, to determine whether there exists a set $V' \in V(G)$ of size ℓ such that V' is both a dominating set

and an independent set is an NP-complete problem (see [11]). However, for a particular class of graphs, we can compute easily such a set V', and thus obtain an explicit bound.

Corollary 4.5. *Let $G = K_{w_1,w_2,\ldots,w_t}$ be a complete multipartite graph on w vertices such that $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_t$. Then, in any strict anonymous secret sharing scheme for G with key set $\mathscr{K}$, the size of the share set $\mathscr{S}$ satisfies*

$$|\mathscr{S}| \geqslant (w - w_1)|\mathscr{K}| + w_1.$$

Proof. For $i = 1,2,\ldots,t$, let $V_i \subseteq V(G)$ be the ith part of G, with $|V_i| = w_i$. It is easy to see that the set V_1 is the minimum size independent set of G that is also a dominating set. □

5. Constructions for anonymous schemes

In this section we discuss briefly some simple constructions for anonymous schemes. Some of these constructions are modifications of previously known constructions. As an illustration, we apply our constructions to access structures based on complete multipartite graphs.

First, we note that Brickell and Stinson [6] showed how to transform any secret sharing scheme for an access structure Γ into a strict anonymous one.

Theorem 5.1. *Suppose that there exists a secret sharing scheme for access structure Γ, having participant set $\mathscr{P}$, key set $\mathscr{K}$ and share set $\mathscr{S}$. Then there exists a strict anonymous scheme for access structure Γ, having key set $\mathscr{K}$ and share set $\mathscr{P} \times \mathscr{S}$.*

We now look at the concept of 'splitting' an access structure, an idea introduced in the context of graph access structures in [6] (note also that splitting is a special case of 'insertion' [17]). Suppose Γ is an access structure for participant set $\mathscr{P}$, and let $\tau : \mathscr{P} \to \mathbb{Z}^+$. For each $P \in \mathscr{P}$, let $P' = \{P\} \times \{1,\ldots,\tau(P)\}$ be a set of $\tau(P)$ participants. Then define $\mathscr{P}' = \bigcup_{P \in \mathscr{P}} P'$ to be a new participant set. For each $B \in \Gamma$, and for each function $\phi : B \to \mathbb{Z}^+$ such that $\phi(P) \leqslant \tau(P)$ for every $P \in B$, let $B_\phi = \{(P, \phi(P)) : P \in B\}$. Take Γ' to consist of all such sets B_ϕ, $B \in \Gamma$. Then we say that Γ' is obtained from Γ by *splitting*.

The following theorem holds.

Theorem 5.2. *Let Γ be an access structure on a set $\mathscr{P}$ of participants, and suppose there exists a strict anonymous scheme for Γ with a key set of size q and a share set of size v. Let Γ' be any access structure obtained by splitting Γ. Then there exists an anonymous scheme for Γ' with a key set of size q and a share set of size v.*

Proof. Let $\mathscr{F}$ be the collection of distribution rules for the scheme realizing Γ. For every $f \in \mathscr{F}$, define a new distribution rule f' for the participants in $\mathscr{P}'$ by the rule $f'(Q) = f(P)$ for every $Q \in P'$. (In terms of the matrix M representing the scheme for Γ, we replace every column P by $\tau(P)$ identical columns indexed by P'.) □

Here are some applications of this idea. Stinson and Vanstone [26] gave the following construction for (optimal) strict anonymous schemes:

Theorem 5.3 (Stinson and Vanstone [26]). *A strict anonymous scheme for a (t,w) threshold structure with a set $\mathscr{K}$ of $(v-t+1)/(w-t+1)$ keys having a set $\mathscr{S}$ of v shares exists if and only if there exists a Steiner system $S(t,w,v)$ that can be partitioned into Steiner systems $S(t-1,w,v)$.*

Applying Theorems 5.2 and 5.3 we obtain the following.

Theorem 5.4. *Let $G = K_{w_1,w_2,\ldots,w_k}$ be a complete multipartite graph on k parts. If there exists a resolvable Steiner system $S(2,k,v)$, then there exists an anonymous secret sharing scheme for G for a set $\mathscr{K}$ of $(v-1)/(k-1)$ keys having a share set of size v.*

Proof. A complete multipartite graph with k parts can be obtained by splitting a complete graph on k vertices (which is a $(2,k)$ threshold access structure). □

Using Theorem 2.1, Theorem 5.4 can be applied for $k = 2, 3$ or 4 if $v \equiv k \bmod k(k-1)$. In the case $k = 2$, this provides a scheme with q keys and $q+1$ shares for an access structure which is the closure of the edge set of a complete bipartite graph, but it is possible to do better using the Phillips–Phillips construction (Theorem 3.1).

In the case of a $(2,w)$ threshold structure, we can construct an anonymous scheme having one more key than a strict anonymous scheme obtained from Theorem 5.3.

Theorem 5.5. *If there exists a resolvable Steiner system $S(2,w,v)$, then there exists an anonymous $(2,w)$ threshold scheme having a key set $\mathscr{K}$ of size $(v-1)/(w-1)+1$ and a share set $\mathscr{S}$ of size v.*

Proof. If a resolvable Steiner system $S(2,w,v)$ exists, then from Theorem 5.3 there exists a strict anonymous scheme with a key set of size $(v-1)/(w-1)$ and a share set $\mathscr{S}$ of size v. Let $\mathscr{F}$ be the family of distribution rules of such a scheme. Let $\infty \notin \mathscr{K}$ be a new key, and define $\mathscr{F}_\infty = \{(x,x,\ldots,x): x \in \mathscr{S}\}$. Consider the family $\mathscr{F}' = \mathscr{F} \cup \mathscr{F}_\infty$. It is easy to check that $\mathscr{F}'$ constitutes a family of distribution rules for an anonymous secret sharing scheme for Γ with a set of $(v-1)/(w-1)+1$ keys having a share set $\mathscr{S}$ of size v. □

Remarks 5.1. The scheme presented in Example 2.1 for the $(2,3)$ threshold structure is based on the previous construction.

In the following theorem, we present a technique to obtain strict anonymous secret sharing schemes for access structures constructed by splitting.

Theorem 5.6. *Let Γ be an access structure on a set $\mathscr{P}$ of participants, and suppose there exists a strict anonymous scheme for Γ with a key set of size q and a share set of size v. Let Γ' be the access structure obtained by splitting Γ using the function τ. Denote $T = \max\{\tau(P): P \in \mathscr{P}\}$. Then there exists a strict anonymous scheme for Γ' with a key set of size q and a share set of size vT.*

Proof. Let $\mathscr{F}$ be the collection of distribution rules for the scheme realizing Γ. Let $\mathscr{S}$ be the share set for the scheme $\mathscr{F}$, and define $\mathscr{S}' = \mathscr{S} \times \{i: 1 \leqslant i \leqslant T\}$. For every $f \in \mathscr{F}$, define a new distribution rule f' for the participants in $\mathscr{P}'$ by the rule $f'(P,i) = (f(P),i)$ for every $P \in \mathscr{P}$, $1 \leqslant i \leqslant \tau(P)$. □

Again, we will apply this construction in the case of complete multipartite graphs.

Theorem 5.7. *Let $G = K_{w_1,w_2,\ldots,w_t}$ be a complete multipartite graph such that $w_1 \leqslant w_2 \leqslant \cdots \leqslant w_k$. Suppose there exist a resolvable Steiner system $S(2,k,v)$. Then, there exists a strict anonymous secret sharing scheme for G with a set $\mathscr{K}$ of $(v-1)/(k-1)$ keys, having a share set of size $w_k v$.*

If $w_1 = w_2 = \cdots = w_k$, then by Corollary 4.5 the scheme is optimal with respect to the size of the share set. For example, in the case $k = 2$, we obtain the following corollary.

Corollary 5.8. *Let G be a complete bipartite graph $K_{w,w}$. Then there exists an optimal strict anonymous scheme for G for any set $\mathscr{K}$ of $q \geqslant 3$ keys, q odd, having $(q+1)w$ possible shares.*

Acknowledgements

C. Blundo's research is supported by the Italian Ministry of University and Research (M.U.S.R.T.) and by the National Council for Research (C.N.R.), and D.R. Stinson's research is supported by NSF grant CCR-9402141. We would like to thank the referees for their careful reading of the manuscript and for their suggestions concerning the presentation of various results in this paper.

References

[1] J.C. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, in: S. Goldwasser, ed., Advances in Cryptology – CRYPTO '88, Lecture Notes in Computer Science, Vol. 403 (Springer, Berlin, 1990) 27–35.

[2] G.R. Blakley, Safeguarding cryptographic keys, Proc. AFIPS 1979 National Computer Conf., Vol. 48, New York (1979) 313–317.

[3] C. Blundo, A. De Santis, L. Gargano and U. Vaccaro, On the information rate of secret sharing schemes, in: E. Brickell, ed., Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science, Vol. 740 (Springer, Berlin, 1993) 149–169.
[4] C. Blundo, A. De Santis, D.R. Stinson and U. Vaccaro, Graph decompositions and secret sharing schemes, J. Cryptology 8 (1995) 39–64.
[5] E.F. Brickell and D.M. Davenport, On the classification of ideal secret sharing schemes, J. Cryptology 4 (1991) 123–134.
[6] E.F. Brickell and D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, J. Cryptology 5 (1992) 153–166.
[7] R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, A note on secret sharing schemes, in: R. Capocelli, A. De Santis and U. Vaccaro, eds., Sequences II: Methods in Communication, Security and Computer Science (Springer, Berlin, 1993) 335–344.
[8] R.M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, J. Cryptology 6 (1993) 157–169.
[9] D. Chen and D.R. Stinson, Recent results on combinatorial constructions for threshold schemes, Australasian J. Combin. 1 (1990) 29–48.
[10] C.J. Colbourn and J.H. Dinitz, eds., CRC Handbook of Combinatorial Designs (CRC Press, Boca Raton, 1996).
[11] M. Garey and D. Johnson, Computers and Intractability: a Guide to the Theory of NP-Completeness, (W.H. Freeman, New York, 1979).
[12] O. Goldreich, S. Micali and A. Wigderson, How to play any mental game, Proc. 19th ACM STOC (1987) 218–229.
[13] H. Hanani, D.K. Ray-Chaudhuri and R.M. Wilson, On resolvable designs, Discrete Math. 3 (1972) 343–357.
[14] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, Proc. Globecom '87, Tokyo, Japan (1987) 99–102.
[15] W.-A. Jackson and K.M. Martin, Combinatorial models for perfect secret sharing schemes, J. Combin. Math. Combin. Comput., to appear.
[16] K. Kurosawa and K. Okada, Combinatorial interpretation of secret sharing schemes, in: J. Pieprzyk and R. Safavi-Naini, eds., Advances in Cryptology – ASIACRYPT '94, Lecture Notes in Computer Science, Vol. 917 (Springer, Berlin, 1995) 55–64.
[17] K.M. Martin, New secret sharing schemes from old, J. Combin. Math. Combin. Comput. 14 (1993) 65–77.
[18] S.J. Phillips and N.C. Phillips, Strongly ideal secret sharing schemes, J. Cryptology 5 (1992) 185–191.
[19] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman' s Schoolgirl Problem, Amer. Math. Soc. Proc. Symp. Pure Math. 19 (1971) 187–204.
[20] P.J. Schellenberg and D.R. Stinson, Threshold schemes from combinatorial designs, J. Combin. Math. Combin. Comput. 5 (1989) 143–160.
[21] A. Shamir, How to share a secret, Comm. ACM 22 (1979) 612–613.
[22] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their application, in: G.J. Simmons, ed., Contemporary Cryptology (IEEE Press, New York, 1991) 441–497.
[23] D.R. Stinson, An explication of secret sharing schemes, Designs, Codes and Cryptography 2 (1992) 357–390.
[24] D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes, in: E. Brickell, ed., Advances in Cryptology – CRYPTO '92, Lecture Notes in Computer Science, Vol. 740 (Springer, Berlin, 1993) 170–184.
[25] D.R. Stinson, Decomposition constructions for secret sharing schemes, IEEE Trans. Inform. Theory 40 (1994) 118–125.
[26] D.R. Stinson and S.A. Vanstone, A combinatorial approach to threshold schemes, SIAM J. Discrete Math. 1 (1988) 230–236.