Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes

(extended abstract)

E. F. Brickell[1]
Sandia National Laboratories
Albuquerque NM 87185

D. R. Stinson[2]
Computer Science and Engineering
University of Nebraska
Lincoln NE 68588

1. Introduction and definitions

Informally, a *secret sharing scheme* is a method of sharing a secret key K among a finite set of participants, in such a way that certain specified subsets of participants can compute a key. Suppose that $\mathbf{P}$ is the set of participants. Denote by Γ the set of subsets of participants which we desire to be able to determine the key; hence $\Gamma \subseteq 2^{\mathbf{P}}$. Γ is called the *access structure* of the secret sharing scheme. It seems reasonable to require that Γ be *monotone*, i.e.

$$\text{if } B \in \Gamma \text{ and } B \subseteq C \subseteq \mathbf{P}, \text{ then } C \in \Gamma.$$

For any $\Gamma_0 \subseteq 2^{\mathbf{P}}$, define the *closure* of Γ_0 to be

$$\text{cl}(\Gamma_0) = \{C: \ B \in \Gamma \text{ and } B \subseteq C \subseteq \mathbf{P}\}.$$

Note that the closure of any set of subsets is monotone.

Let $\mathbf{K}$ be a set of q elements called *keys*, and let $\mathbf{S}$ be a set of s elements called *shares*. Suppose a dealer D wants to a share the secret key $K \in \mathbf{K}$ among the participants in $\mathbf{P}$ (we will assume

[1] This work performed at Sandia National Laboratories and supported by the U. S. Department of Energy under contract number DE-AC04-76DP00789

[2] Research supported by NSERC operating grant A9287 and by the Center for Communication and Information Science, University of Nebraska

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 242-252, 1991.

that $D \notin \mathbf{P}$). He does this by giving each participant a share. We say that the scheme is a *perfect* scheme with access structure Γ if the following two properties are satisfied:

1) if a subset B of participants pool their shares, where $B \in \Gamma$, then they can determine the value of K.

2) if a subset B of participants pool their shares, where $B \notin \Gamma$, then they can determine nothing about the value of K (in an information-theoretic sense), even with infinite computational resources.

We will depict a secret sharing scheme as a matrix M, as was done in [5]. There will be $|\mathbf{P}| + 1$ columns. The first column of M will be indexed by D, and the remaining columns are indexed by the members of $\mathbf{P}$. In any row of M, we place a value of the key K in the column D, and a possible list of shares corresponding to K in the remaining columns. When D wants to distribute shares corresponding to a key K, he will choose at random a row of M having K in column D, and distribute the shares in that row to the participants.

With this matrix representation, it is easy to describe conditions 1) and 2) above. Condition 1) becomes the following.

1') if $B \in \Gamma$ and $M(r, b) = M(r', b)$ for all $b \in B$, then $M(r, D) = M(r', D)$.

We will replace Condition 2) by a condition which Brickell and Davenport [5] call "having no probabilistic information regarding the key". This condition is the following:

2') if $B \notin \Gamma$ and $f\colon B \to \mathbf{S}$ is any function, then there exists a non-negative integer $\lambda(f, B)$ such that

$$|\{r\colon \{(b, M(r, b))\colon b \in B\} = \{(b, f(b))\colon b \in B\} \text{ and } M(r, D) = K\}| = \lambda(f, B),$$

independent of the value of K.

The *information rate* of the secret sharing scheme is defined to be $\rho = \log_2 q / \log_2 s$. It is not difficult to see that $q \leq s$ in a perfect scheme, so the information rate $\rho \leq 1$. If a secret sharing scheme is to be practical, we do not want to have to distribute too much secret information as shares. Consequently, we want to make the information rate as close to 1 as possible. A perfect secret sharing scheme with information rate $\rho = 1$ is called *ideal*. In Example 1.1, we depict an ideal secret sharing scheme.

Example 1.1 Let $\mathbf{P} = \{a, b, c\}$ and let $\Gamma = \left\{ \{a, b\}, \{b, c\}, \{a, b, c\} \right\}$. The following is a $\mathrm{PS}(\Gamma, 1, 3\}$.

D	a	b	c
1	1	2	1
1	2	0	2
1	0	1	0
2	1	0	1
2	2	1	2
2	0	2	0
0	1	1	1
0	2	2	2
0	0	0	0

Note that if a has share s_a and b has share s_b, then they can compute the key as $s_b - s_a$ (modulo 3). Similarly, b and c can compute the key as $s_b - s_c$ (modulo 3). However, a and c together have no information regarding the key, since $s_a = s_c$ in every row.

We will use the notation $\mathrm{PS}(\Gamma, \rho, q)$ to denote a perfect secret sharing scheme with access structure Γ and information rate ρ for a set of q keys.

In the special case where the access structure $\Gamma = \{B \subseteq \mathbf{P}\colon |B| \geq t\}$, then the secret sharing scheme is called a *(t, w)-threshold scheme*, where $w = |\mathbf{P}|$. Threshold schemes have been extensively studied in the literature; see Simmons [9] for a comprehensive bibliography.

Secret sharing schemes for general access structures were first studied by Ito, Saito and Nishizeki in [6]. They proved that *any* monotone access structure can be realized by a perfect secret sharing scheme. A more efficient construction was given by Beneloh and Leichter in [1]. In both these constructions, however, the information rate is exponentially small as a function of $|\mathbf{P}|$.

Some constructions for ideal schemes were given by Brickell [4]. More recently, ideal schemes were characterized by Brickell and Davenport [5] in terms of matroids.

2. Ideal secret sharing schemes

In this section, we will discuss ideal secret sharing schemes in the case where the access structure consists of the closure of a graph. In this paper, graphs do not have loops or multiple edges; a graph with multiple edges will be termed a *multigraph*. If G is a graph, we denote the vertex set of G by $V(G)$ and the edge set by $E(G)$. 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* $K_{n_1,n_2,\dots,n_t}$ is a graph on $\sum_{i=1}^{t} n_i$ vertices, in which the vertex set is partitioned into subsets of size n_i ($1 \le i \le t$), such that vw is an edge if and only if v and w are in different subsets of the partition. An alternative way to characterize a complete multipartite graph is to say that the complementary graph is a vertex-disjoint union of cliques.

For a graph G, define $PS(G, \rho, q)$ to be $PS(\Gamma, \rho, q)$, where $\Gamma = cl(E(G))$.

The following result characterizing which graphs admit ideal secret sharing schemes was proved in [5].

Theorem 2.1 [5, Theorems 4 and 5] Suppose G is a connected graph. Then there exists a $PS(G, 1, q)$ for some q if and only if G is a complete multipartite graph.

Theorem 2.1 requires that G be connected. The cases when G is not connected are easily handled by the following easy observation.

Theorem 2.2 Suppose G is a graph having as its connected components G_i, $1 \le i \le t$. Suppose that there is a $PS(G_i, \rho, q)$, $1 \le i \le t$. Then there is a $PS(G, \rho, q)$.

We can easily prove the constructive half of Theorem 2.1 by using a couple of simple constructions. Suppose G is a graph and $v \in V(G)$. We define a graph $G(v)$ by replacing v by two non-adjacent vertices v_1 and v_2, such that v_iw is an edge of $G(v)$ if and only if vw is an edge of G ($i = 1, 2$). We say that $G(v)$ is constructed from G by *splitting* v.

Theorem 2.3 Suppose G is a graph and there exists a PS(G, ρ, q). Then for any vertex v of G, there exists a PS($G(v)$, ρ, q).

Proof: Replace column v of the matrix M by two identical columns v_1 and v_2.

The next theorem generalizes the Shamir construction for a (2, 2)-threshold scheme [7]. It uses a structure from combinatorial design theory called an orthogonal array. 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.

Theorem 2.4 Suppose t is a positive integer, and there exists an orthogonal array $OA(t + 1, q)$. Then there is a PS(K_t, 1, q).

Proof: We will use the $OA(t + 1, q)$ as the matrix M representing the secret sharing scheme. The first column is indexed by D, and the remaining t columns are indexed by the participants. Let P_i and P_j be two participants. In the two corresponding columns, every ordered pair of shares occurs exactly once. Hence, property 1') is satisfied. If we consider any one participant P_i, any share $s = f(P_i)$, and any key K, there is a unique row of M such that s occurs in column P_i and K occurs in column D. Hence, property 2') is satisfied with $\lambda(f, P_i) = 1$.

Corollary 2.5 Suppose t is a positive integer, q is a prime power, and $q \geq t$. Then there is a PS(K_t, 1, q).

Proof: It is well-known that an $OA(t + 1, q)$ exists if q is a prime power and $q \geq t$ (e.g., see [2]).

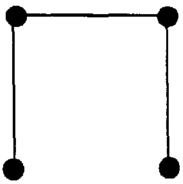
We can now prove the constructive half of Theorem 2.1 as a corollary of these constructions.

Corollary 2.6 [5, Theorem 5] Suppose q is a prime power and $q \geq t$. Then there is a PS($K_{n_1,n_2,\ldots,n_t}$, 1, q).

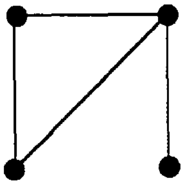
Proof: Start with a PS(K_t, 1, q) and split vertices until $K_{n_1,n_2,\ldots,n_t}$ is obtained.

If we consider the possible graphs on at most four vertices, we find that all of them admit ideal secret sharing schemes, with two exceptions. We have the following consequence of the Theorems 2.1 and 2.2.

Theorem 2.7 If G is a graph and $|V(G)| \leq 4$, then there exists a PS(G, 1, q) for some q, unless G is isomorphic to one of the following two graphs:



P_3



H

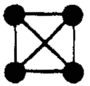
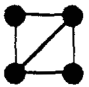
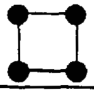
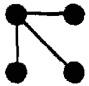
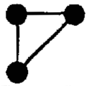
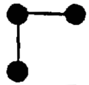
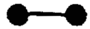
Remark: It was first shown by Beneloh and Leichter [1] that there does not exist a PS(P_3, 1, q), where P_3 is the path of length 3, for any q.

In fact, we can be more precise about the values of q admitted in Theorem 2.7.

Theorem 2.8 If G is a connected graph, $|V(G)| \leq 4$, and G is not isomorphic to P_3 or H, then there exists a PS(G, 1, q) for all integers $q \in Q(G)$, where $Q(G)$ is defined in Table 1.

Proof: It is known that there exists an $OA(5, q)$ if $q \geq 4$, $q \neq 6$, 10; there exists an $OA(4, q)$ if $q \geq 3$, $q \neq 6$; and there exists an $OA(3, q)$ if $q \geq 2$ (see [2] for proofs).

Table 1

G	$\lvert V(G) \rvert$	G^c	$Q(G)$
	4		$\{q\colon\ q \geq 5, q \neq 6, 10\}$
	4	K_2	$\{q\colon\ q \geq 3, q \neq 6\}$
	4	$K_2 \cup K_2$	$\{q\colon\ q \geq 2\}$
	4	K_3	$\{q\colon\ q \geq 2\}$
	3		$\{q\colon\ q \geq 3, q \neq 6\}$
	3	K_2	$\{q\colon\ q \geq 2\}$
	2		$\{q\colon\ q \geq 2\}$

3. Improved lower bounds on the information rate

We now turn to the construction of perfect secret sharing schemes in the cases where ideal schemes do not exist. First, we give a construction that shows that the existence of a secret sharing scheme PS(Γ, ρ, q) for a single value of q implies the existence of an infinite class of schemes with the same information rate.

Theorem 3.1 Suppose there is a PS(Γ, ρ, q_1) and a PS(Γ, ρ, q_2). Then there is a PS(Γ, ρ, q_1q_2).

Corollary 3.2 Suppose there is a PS(Γ, ρ, q). Then, for any positive integer n, there is a PS(Γ, ρ, q^n).

If G is a graph, then G_1 is said to be a *subgraph* of G if $V(G) \subseteq V(G_1)$ and $E(G) \subseteq E(G_1)$. If $V_1 \subseteq V(G)$, then we define the graph $G[V_1]$ to have vertex set V_1 and edge set $\{uv \in E(G), u, v \in V_1\}$. We say that $G[V_1]$ is an *induced subgraph* of G. The following theorem is obvious.

Theorem 3.3 Suppose G is a graph and G_1 is an induced subgraph of G. If there is a $PG(G_1, \rho, q)$, then there exists a $PS(G_1, \rho, q)$.

Next, we prove some powerful "decomposition" constructions.

Theorem 3.4 Suppose G is a graph, and G_1 and G_2 are subgraphs of G such that $E(G) = E(G_1) \cup E(G_2)$. Suppose that there is a $PS(G_1, \rho_1, q)$ and a $PS(G_2, \rho_2, q)$. Then there is a $PS(G, \rho, q)$, where

$$\rho = \frac{\rho_1 \rho_2}{\rho_1 + \rho_2}.$$

This theorem can be generalized as follows.

Theorem 3.5 Suppose G is a graph and $G_1, \ldots, G_t$ are all subgraphs of G, such that each edge of G occurs in at least one of the G_i's. For $1 \leq i \leq t$, suppose that there is a $PS(G_i, \rho_i, q)$. For every vertex v, define

$$\rho(v) = \frac{1}{\sum_{\{i:\ v \in G_i\}} \frac{1}{\rho_i}}.$$

Then there is a $PS(G, \rho, q)$, where $\rho = \min\{\rho(v):\ v \in V(G)\}$.

Corollary 3.6 Suppose G is any graph with maximum degree d, and $q \geq 2$ is any integer. Then there is a $PS(G, 1 / d, q)$.

Proof: Define each G_i to be an edge of G, and apply Theorem 3.5.

Remark: Corollary 3.6 can also be proved by the "monotone circuit" construction of Beneloh and Leichter [1].

We can now obtain schemes for the two graphs P_3 and H from the previous constructions.

Corollary 3.7 There exist schemes PS(P_3, 0.5, q) and PS(H, 0.5, q) for all $q \geq 2$.

Proof: Existence of a scheme PS(P_3, 0.5, q) follows from Corollary 3.6. Existence of PS(H, 0.5, q) follows from decomposing H into two edge-disjoint paths of length two, each of which admits an ideal secret sharing scheme, and applying Theorem 3.5.

We now establish a general lower bound improving that of Corollary 3.6.

Theorem 3.8 Suppose G is a graph of maximium degree d, and denote $e = \lceil d / 2 \rceil$. Then there is a constant $\rho \geq 1 / (e + 1)$ such that there exists a PS(G, ρ, q) for all $q \geq 2$.

Proof: Let x_i $(1 \leq i \leq 2t)$ be the vertices in V(G) having odd degree (any graph has an even number of vertices of odd degree). Construct G' from G by adding t new edges $x_{2i-1}\, x_{2i}$ $(1 \leq i \leq t)$. Observe that G' may contain edges of multiplicity two, in which case it is a multigraph. Every vertex of G' has even degree; hence G' is Eulerian. Let C be a (directed) Eulerian tour of G'. For every vertex $v \in$ V(G) define G_v to consist of the edges of $C \cap$ E(G) for which v is the head. Then the subgraphs G_v ($v \in$ V(G)) form an edge-decomposition of G. Also, each G_v is isomorphic to a complete bipartite graph K_{1,n_0}, where

$n_0 = d_0 / 2$, if v has degree d_0 in G and d_0 is even
$n_0 = \lceil d_0 / 2 \rceil$ or $\lfloor d_0 / 2 \rfloor$, if v has degree d_0 in G and d_0 is odd.

Hence, each G_v admits an ideal secret sharing scheme for any $q \geq 2$ (Corollary 2.6). Now, apply Theorem 3.5. For every vertex $v \in$ V(G), we have

$\rho(v) = 1 / (e_0 + 1)$, if v has even degree d_0 in G and $e_0 = d_0 / 2$,
$\rho(v) = 1 / e_0$ or $1 / (e_0 + 1)$, if v has odd degree d_0 in G and $e_0 = \lceil d_0 / 2 \rceil$.

It follows that the resulting secret sharing scheme has rate $\rho = 1 / e$ or $1 / (e + 1)$, where G has maximum degree d and $e = \lceil d / 2 \rceil$. Such a scheme can be constructed for any $q \geq 2$.

The last topic of this section is a direct construction for a secret sharing scheme for C_6, the cycle of size 6. Note that there is no ideal scheme in this case.

Example 3.1 The following is a PS(C_6, $\log_3 2$, 2}, where V(C_6) = $\{a, b, c, d, e, f\}$ and E(C_6) = $\big\{ \{a, b\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, a\} \big\}$.

D	a	b	c	d	e	f
0	0	0	1	1	2	2
0	0	0	2	2	1	1
0	1	1	2	2	0	0
0	1	1	0	0	2	2
0	2	2	0	0	1	1
0	2	2	1	1	0	0
1	0	1	1	2	2	0
1	0	2	2	1	1	0
1	1	2	2	0	0	1
1	1	0	0	2	2	1
1	2	0	0	1	1	2
1	2	1	1	0	0	2

Note that if a has share s_a and b has share s_b, then they can compute the key to be 0 if $s_b = s_a$, and 1 otherwise. However, a and c together have no information regarding the key, since for every ordered pair (s_b, s_c) that occurs, there is exactly one row where the key is 0 and one row where the key is 1. The analysis for other pairs of participants is similar to these arguments. The information rate $\rho = \log_2 2 / \log_2 3 = \log_3 2 \approx 0.6309298$.

Remark: Example 3.1 also provides us with a PS(P_3, $\log_3 2$, 2}, since P_3 is an induced subgraph of C_6.

References

1. J. Beneloh and J. Leichter, *Generalized secret sharing and monotone functions*, in "Advances in Cryptology CRYPTO '88 Proceedings", Lecture Notes in Computer Science 403 (1990), 27-35.

2. Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Zurich, 1985.

3. G. R. Blakley, *Safeguarding cryptographic keys*, Proc. National Computer Conference, vol. 48, AFIPS Conference Proceedings 48 (1979), 313-317.

4. E. F. Brickell, *Some ideal secret sharing schemes* , J. Combin. Math. and Combin. Comput. 6 (1989), 105-113.

5. E. F. Brickell and D. M. Davenport, *On the classification of ideal secret sharing schemes*, J. Cryptology, to appear.

6. M. Ito, A. Saito and T. Nishizeki, *Secret sharing scheme realizing general access structure*, Proc. IEEE Globecom '87, Tokyo, Japan, 1987, pp. 99-102.

7. A. Shamir, *How to share a secret*, Commun. of the ACM 22, (1979), 612-613.

8. P. J. Schellenberg and D. R. Stinson, *Threshold schemes from combinatorial designs*, J. Combin. Math. and Combin. Comput. 5 (1989), 143-160.

9. Gustavus J. Simmons, *Robust shared secret schemes or "how to be sure you have the right answer even though you don't know the question"*, Congressus Numer. 68 (1989), 215-248.

10. D. R. Stinson and S. A. Vanstone, *A combinatorial approach to threshold schemes*, SIAM J. on Discrete Math. 1 (1988), 230-236.