On the Classification of Ideal Secret Sharing Schemes

(Extended Abstract)

Ernest F. Brickell
Daniel M. Davenport

Sandia National Laboratories *
Albuquerque, NM 87185

Abstract

In a secret sharing scheme, a dealer has a secret key. There is a finite set P of participants and a set Γ of subsets of P. A secret sharing scheme with Γ as the access structure is a method which the dealer can use to distribute shares to each participant so that a subset of participants can determine the key if and only if that subset is in Γ. The share of a participant is the information sent by the dealer in private to the participant. A secret sharing scheme is ideal if any subset of participants who can use their shares to determine any information about the key can in fact actually determine the key, and if the set of possible shares is the same as the set of possible keys. In this paper, we show a relationship between ideal secret sharing schemes and matroids.

1 Introduction

In a secret sharing scheme, a dealer has a key. There is a finite set P of participants and a set Γ of subsets of P. A secret sharing scheme with Γ as the access structure is a method which the dealer can use to distribute shares to each participant so that a subset of participants can determine the key if and only if that subset is in Γ. A secret sharing scheme is said to be *perfect* if any subset of participants who can use their shares to determine any information about the key can in fact actually determine the key. The *share* of a participant is the information sent by the dealer in private to the participant.

In any practical implementation of a secret sharing scheme, it is important to keep the size of the shares as small as possible. The reason for this is obvious. The most

*This work performed at Sandia National Laboratories and supported by the U.S. Department of Energy under contract No. DE-AC04-76DP00789.

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 278-285, 1990.

secure method for a participant to store a share is in his own memory. However, if his share is too large, he will be inclined to write down information which will help him to remember his share. This, of course, will degrade the security of the scheme. This paper deals with secret sharing shemes in which the shares are as small as possible, i.e. the shares are the same size as the keys.

Let $\mathcal{K}$ be the set of keys and let S be the set of shares used in a secret sharing scheme. The *information rate* for the secret sharing scheme is defined to be $\log_2 |\mathcal{K}| / \log_2 |S|$. A perfect secret sharing scheme is said to be *ideal* if it has information rate 1.

The first constructions of perfect secret sharing schemes were the threshold schemes of Blakley [2] and Shamir [5]. In a threshold scheme, there is a threshold t such that the access structure is $\Gamma = \{A \subseteq P \ : \ |A| \geq t\}$.

A set of subsets Γ of a set P is said to be *monotone* if $B \in \Gamma$ and $B \subseteq C$ implies that $C \in \Gamma$ for any $B, C \subseteq P$. Ito, Saito, and Nishisehi [4], and also Benaloh and Leichter [1] showed that for any monotone set of subsets Γ of P, there exists a perfect secret sharing scheme with Γ as the access structure. However, for both the ISN and the BL constructions, the information rate could be exponentially small in $|P|$.

The schemes of Blakley and Shamir can be implemented so that they are ideal secret sharing schemes. Benaloh and Leichter [1], Brickell [3], and Simmons [6] have constructed ideal secret sharing schemes for other access structures.

The main contribution of the current paper is to give a description of ideal secret sharing schemes in terms of classical combinatorial objects by showing a direct relationship between ideal secret sharing schemes and matroids.

In order to make the definitions more precise, we will define a secret sharing scheme to be a finite matrix M in which no two rows are identical. We will identify the columns of M as the set of participants P and will use $M(r,p)$ to denote the entry of M in row r and column p. We will denote the first column as p_0 and will assume that p_0 always receives the key as his share. It is sometimes useful to think of this special participant p_0 as the dealer. For $p \in P$, let $S(p) = \{M(r,p) \mid r$ is a row in $M\}$. That is, $S(p)$ is the set of the elements occurring in column p and $S(p_0) = \mathcal{K}$. The dealer can distribute a key $\alpha \in S(p_0)$ by picking a row r of the matrix in which $M(r,p_0) = \alpha$ and using $M(r,p)$ as the share for participant p for each $p \in P$. We assume that the matrix is public knowledge, but that the dealer's choice of r is private.

Let $A \subseteq P$. Each participant $a \in A$ receives a share, say α_a, from the dealer. If the participants in A pool their information, they will know that the dealer picked a row r in which $M(r,a) = \alpha_a$ for each $a \in A$. It is now easy to define the access structure Γ. A subset $A \subseteq P$ will be in Γ if and only if any two rows r and $\hat{r}$ such that $M(r,a) = M(\hat{r},a)$ for all $a \in A$ also satisfy $M(r,p_0) = M(\hat{r},p_0)$.

Given a subset $A \subseteq P$ and a participant $b \in P$ with $b \notin A$, we will say that A has *no information* about the share given to b, denoted $A \not\rightarrow b$, if for all rows r of M and $\beta \in S(b)$ there is a row r' such that $M(r,a) = M(r',a)$ for all $a \in A$, and $M(r',b) = \beta$. Otherwise, we will say that A has *some information* about b, and denote this by $A \rightarrow b$. We will say that A *knows* the share given to b, denoted by $A \Rightarrow b$ if all rows that are identical on the participants in A are also identical on b.

Then $\Gamma = \{A \subseteq P \mid A \Rightarrow p_0\}$ is the collection of access sets.

A secret sharing scheme is *perfect* iff for all subsets $A \subseteq P$, $A \rightarrow p_0$ implies that $A \Rightarrow p_0$. A secret sharing scheme is *ideal* iff it is perfect and $|S(p)| = |S(p_0)|$ for all $p \in P$. Thus if a secret sharing scheme is ideal, we will assume WLOG that $S(p) = S(p_0)$ for all $p \in P$ and we will denote $S(p)$ as simply S.

Let Γ_m denote the set of minimal elements of Γ. If there is a participant $p \in P$ such that p is not contained in any subset in Γ_m, then this participant is not needed since there is never a case in which his share is useful in determining the key. It is not interesting to study secret sharing schemes in which some participants receive useless shares. Therefore, we will say that the secret sharing scheme is *connected* if every participant $p \in P$ is contained in some subset in Γ_m, and for the remainder of this paper, will only consider connected secret sharing schemes.

For M an ideal secret sharing scheme, let $D(M) = \{A \subseteq P \mid \text{there exists } y \in A \text{ such that } A \backslash y \Rightarrow y\}$. Intuitively, a set of participants is in $D(M)$ if there is a dependency among them.

Before we state the main results of this paper, we need to introduce the definitions of matroids and nearfields.

Matroids are well studied combinatorial objects (see for example Welsh [8]). A matroid $\mathcal{T} = (V, \mathcal{I})$ is a finite set V and a collection $\mathcal{I}$ of subsets of V such that **(I1)** through **(I3)** are satisfied.

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $X \in \mathcal{I}$ and $Y \subseteq X$ then $Y \in \mathcal{I}$.

(I3) If X,Y are members of $\mathcal{I}$ with $|X| = |Y| + 1$ there exists $x \in X \backslash Y$ such that $Y \cup \{x\} \in \mathcal{I}$.

The elements of V are called the *points* of the matroid and the sets $\mathcal{I}$ are called *independent sets*. A *dependent set* of a matroid is any subset of V that is not independent. The minimal dependent sets are called *circuits*. A matroid is said to be *connected* if for any two elements, there is a circuit containing both of them.

A *right nearfield* is a set R with distinguished elements 0 and 1 and binary operations $+$ and $\cdot$ such that $(R, +)$ is an Abelian group, $(R\backslash 0, \cdot)$ is a group, and $(R, +, \cdot)$ is right distributive (i.e. $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$). If a right nearfield is also left distributive then it is a field. When R is finite its cardinality is always a power of a prime (see [7]). The nearfields we will consider are finite. A right near vector space and its dot product are defined analogously to a vector space only defined over a right nearfield instead of a field. A vector v in a right near vector space V is said to be *dependent* on a set A of vectors iff for every vector $u \in V$, if $u \cdot a = 0$ for all $a \in A$ then $u \cdot v = 0$. In the case that the right nearfield is actually a field, this definition of dependence is equivalent to stating that a vector v is dependent on a set A of vectors iff v is a linear combination of the vectors in A. A set A of vectors is said to be a *dependent set* if there exists $a \in A$ such that a is dependent on $A\backslash a$. A matroid is representable over a right nearfield if there is a dependence preserving injection from the points of the matroid into the set of vectors of a right near vector space.

In this paper, we prove the following two theorems which together almost characterize ideal secret sharing schemes.

Theorem 1 *Let M be a connected ideal secret sharing scheme. Then the sets $D(M)$ are the dependent sets of a connected matroid.*

Theorem 2 *Let $\mathcal{T} = (V, \mathcal{I})$ be a connected matroid representable over a nearfield. Let $v_0 \in V$. Then there exists a connected ideal secret sharing scheme M such that $p_0 = v_0$, $P = V$, and $D(M) =$ the dependent sets of $\mathcal{T}$.*

We say that this almost characterizes ideal secret sharing schemes because there may be connected matroids that are not representable over any nearfield, and for any such matroids, we do not know if there exist corresponding ideal secret sharing schemes.

Another interesting result that can be easily proven from the methods used in proving Theorem 1 is the following.

Theorem 3 *Let M be a connected ideal secret sharing scheme. Let $A \subseteq P$ and $b \in P$. If $A \rightarrow b$, then $A \Rightarrow b$.*

This theorem shows that any participant in a connected ideal secret sharing scheme can be thought of as the special participant, p_0.

There is an alternate definition for ideal secret sharing that at first glance appears to be a weaker definition. Let $A \subseteq P$ and $b \in P \backslash A$. We will say that A has *no probabilistic information* about the share given to b, denoted $A \not\rightsquigarrow b$, if for all rows r of M, there exists an integer n such that for all $\beta \in S(b)$, there are exactly n distinct rows $r'_1, \cdots, r'_n$ such that for $1 \leq i \leq n, M(r, a) = M(r'_i, a)$ for all $a \in A$ and $M(r'_i, b) = \beta$. Otherwise we will say that A has *probabilistic information* about the share given to b and denote this by $A \rightsquigarrow b$.

It would be reasonable to define a perfect secret sharing scheme as one in which $A \rightsquigarrow p_0$ implies that $A \Rightarrow p_0$. But the next theorem shows that at least for connected secret sharing schemes with information rate 1, this definition would be equivalent to our original definition.

Theorem 4 *Let M be a connected ideal secret sharing scheme. Then $A \rightsquigarrow p_0$ implies that $A \Rightarrow p_0$.*

In the next section, we consider a special case in which we are able to establish necessary and sufficient conditions for the existence of an ideal secret sharing scheme. The proofs of the general case will not be presented in this extended abstract, but will be contained in the final paper. We conclude the extended abstract with some open problems in Section 3.

2 Example: The Rank 2 Case

In this section we will prove Theorems 1 and 2 in a special case that is much easier to prove and more intuitive than the general case. But first we need some lemmas that will hold for the general case as well.

Let M be a connected ideal secret sharing scheme. Let $q = |S|$. For $A \subseteq P$, let $M(r, A)$ be the row r in M restricted to the columns indexed by A and define $s(A) = \{M(r, A) : r \text{ is a row of } M\}$. That is, $s(A)$ is the set of distinct entries in M under A. Let $\sharp A = |s(A)|$.

Lemma 1 *Let $A \subseteq P$ and $p \in P$. If $A \Rightarrow p$, then $\sharp A = \sharp(A \cup p)$.*

Proof: If $\sharp(A \cup p) > \sharp A$, there exists rows r_1 and r_2 such that $M(r_1, a) = M(r_2, a)$ for all $a \in A$ and $M(r_1, p) \neq M(r_2, p)$. But this contradicts $A \Rightarrow p$. □

Lemma 2 *Let $A \subseteq P$ and $p \in P$. Suppose $A \not\Rightarrow p_0$ and $A \cup p \Rightarrow p_0$. Then $A \cup p_0 \Rightarrow p$.*

Proof: Define a function $\phi : S \rightarrow S$ by $\phi(\beta) = \gamma$ iff there exists a row r such that $M(r, a) = M(r_1, a)$ for all $a \in A$, and $M(r, p) = \beta$ and $M(r, p_0) = \gamma$. Since $(A \cup p) \Rightarrow p_0$, this function is well defined. Since $A \not\rightarrow p_0$, ϕ must be onto and hence 1-1. □

For a secret sharing scheme M, let $\hat{P} = \{p \in P \mid p \not\Rightarrow p_0\}$. Let $G(M)$ be a graph with vertices the participants in $\hat{P}$ and with $p_1, p_2 \in \hat{P}$ joined with an edge iff $\{p_1, p_2\} \in \Gamma$.

A connected ideal secret sharing scheme, M, is said to have rank 2 iff (S1) - (S3) are satisfied.

(S1) There exists a set in Γ_m of cardinality 2.

(S2) All sets in Γ_m have cardinality 1 or 2.

(S3) $G(M)$ is connected.

We then have the following Theorem.

Theorem 5 *Let M be a rank 2 connected ideal secret sharing scheme. Let G' be the complementary graph of $G(M)$. Then G' is a disjoint union of cliques.*

Proof: Let $\{p_1, p_2\} \in \Gamma_m$. If there exists α_1, α_2 both in S such that there is no row r of M with $M(r, p_i) = \alpha_i$ for $i = 1, 2$, then $p_1 \rightarrow p_2$. Hence, $p_1 \rightarrow p_0$ and thus $p_1 \Rightarrow p_0$. Contradiction. Thus, $\sharp\{p_1, p_2\} = q^2$.

Let $A \subseteq P$ be maximal set such that $\sharp A = q^2$ and $\{p_1, p_2\} \subseteq A$. By Lemma 1, $p_0 \in A$ and $P \backslash \hat{P} \subseteq A$. Suppose $P \backslash A \neq \emptyset$. Since $G(M)$ is connected, there exists $b \in P \backslash A$ and $a \in A$ such that $\{a, b\} \in \Gamma$. By Lemma 2, $\{a, p_0\} \Rightarrow b$. Since $\{a, p_0\} \in A$, $\sharp A = \sharp(A \cup b)$. Contradiction. Thus $\sharp P = q^2$.

Suppose $\{a, b\} \subseteq \hat{P}$ and $\{a, b\} \notin \Gamma$. Let r be a row of M. Then for all $\beta \in S$, there exists a row r_β such that $M(r_\beta, a) = M(r, a)$, $M(r_\beta, b) = M(r, b)$ and $M(r_\beta, p_0) = \beta$.

Thus, $q\sharp\{a,b\} = \sharp\{a,b,p_0\} \leq q^2$. Since $\sharp a = q$, $\sharp\{a,b\} = q$. Since $\sharp b$ is also q, we must have $a \Rightarrow b$. Suppose now that $\{a,b,c\} \subseteq \hat{P}$ and $\{a,b\} \not\in \Gamma$ and $\{b,c\} \not\in \Gamma$. Since $a \Rightarrow b$ and $b \Rightarrow c$ implies $a \Rightarrow c$, we also have $\{a,c\} \not\in \Gamma$. Theorem 5 now follows. □

The converse to Theorem 5 is also true.

Theorem 6 *Let G' be a graph which is a disjoint union of cliques. Then there exists a rank 2 connected ideal secret sharing scheme M, with $P = V(G') \cup p_0$ such that $G(M) =$ complement of G'.*

Proof: Let C be the set of distinct components of G'. Let n be the number of components of G'. Let $\hat{C} = C \cup p_0$. Let $\hat{S} = (\hat{C}, S, \hat{M})$ be an ideal 2 out of n threshold scheme with $|S| = q$. Using the Shamir construction, such a threshold scheme exists for all prime power q such that $q > n$. Let M be a matrix with the same number of rows as $\hat{M}$ and with columns indexed by the vertices of G'. For a vertex $v \in G'$ contained in component $c \in C$, and r a row of $\hat{M}$, let $M(r,v) = \hat{M}(r,c)$. Let $M(r,p_0) = \hat{M}(r,p_0)$ for all rows r of $\hat{M}$. It is straightforward to check that M is a rank 2 connected ideal secret sharing scheme. □

These two theorems now make it easy to prove Theorems 1 and 2 for this special case.

For M a rank 2 connected ideal secret sharing scheme, let $\mathcal{I}(M) = \{\emptyset\} \cup \{p \mid p \in P\} \cup \{\{p_1,p_2\} \mid p_1 \Rightarrow p_0 \text{ and } p_2 \not\Rightarrow p_0\} \cup \{\{p_1,p_2\} \mid \{p_1,p_2\} \subseteq \Gamma_m\}$.

It is easy to see that $\mathcal{I}(M) = 2^P \backslash D(M)$ (where 2^P is the set of all subsets of P).

Theorem 7 *Let M be a rank 2 connected ideal secret sharing scheme. Then the sets $D(M)$ are the dependent sets of a connected matroid.*

Proof: We need to show that the set $\mathcal{I}(S)$ satisfies (I1) - (I3). Conditions (I1) and (I2) are trivially satisfied. The same applies to (I3) if $X = \emptyset$ or $X \subset Y$. Thus assume that $|X| = 1$ and $X \not\subseteq Y$. Let $X = \{x\}$ and $Y = \{y_1, y_2\}$. WLOG, we may assume that $y_1 \subseteq \hat{P}$. If $x \in P\backslash\hat{P}$, then $\{x, y_1\} \subseteq \mathcal{I}(S)$. If $x \not\in P\backslash\hat{P}$ and $y_2 \in P\backslash\hat{P}$, then $\{x, y_2\} \in \mathcal{I}(S)$. So we can assume that $x, y_1, y_2, \in \hat{P}$. Since $(y_1, y_2) \in E(G)$, then by Theorem 5, for $i = 1$ or 2, $(x, y_i) \in E(G)$ and so $\{x, y_i\} \in \mathcal{I}(S)$. □

For a set $X \in V$, the rank of X, $\rho(X)$ is defined as

$$\rho(X) = \max\{|A| \ : \ A \subseteq X, A \in \mathcal{I}\}.$$

Theorem 8 *Let $\mathcal{T} = (V, \mathcal{I})$ be a rank 2 connected matroid. Let $v_0 \in V$. Then there exists a connected ideal secret sharing scheme M such that $p_0 = v_0$, $P = V$, and $D(M) =$ the dependent sets of $\mathcal{T}$.*

Proof: Let $\hat{V} = \{v \in V \mid \{v, v_0\} \in \mathcal{I}\}$. Let G be the graph on $\hat{V}$ such that $\{u,v\}$ is an edge of G iff $\{u,v\} \in \mathcal{I}$. From (I3), it follows that the complement of G is a disjoint union of cliques. By Theorem 5, there exists a rank 2 connected ideal secret sharing scheme $\hat{M}$, with $\hat{P} = \hat{V} \cup p_0$ such that $G(\hat{M}) = G$. Let M be the matrix with columns $P = \hat{P} \cup V\backslash\hat{V}$ and with $M(r,p) = \hat{M}(r,p)$ for all $p \in \hat{P}$

and $M(r,p) = \hat{M}(r,p_0)$ for all $p \in P \setminus \hat{P}$. It is straightforward to check that M is a connected ideal secret sharing scheme and the sets $D(M)$ are exactly the dependent sets of $\mathcal{T}$. □

Thus in the rank 2 case, we did not need the condition used in Theorem 2 that the matroid was representable over a nearfield and therefore we were able to completely characterize the connected ideal secret sharing schemes. One possible reason why we were successful in this case but not in the general case is that all rank 2 matroids are representable over fields.

3 Open Questions

The most obvious open question is to determine if Theorem 2 is still true if the condition of the matroid being representable over a nearfield is removed.

There are several other open questions which could also be addressed.

1. Characterize the perfect secret sharing schemes that have a fixed information rate.
2. Characterize the perfect secret sharing schemes that have an information rate that is at least $1/(\text{polynomial in } |P|)$.
3. Find a nontrivial lower bound on the information rate of all perfect secret sharing schemes.
4. Find an algorithm that given a secret sharing scheme, will determine the smallest information rate that could be used to implement that scheme.

Yao [9] has made some progress on problem 2. He has shown that if trap door functions exist, then any set Γ which can be recognized by a polynomial (in $|P|$) size monotone circuit can be the access structure of a secret sharing scheme in which the information rate is at least $1/(\text{polynomial in } |P|)$.

4 Acknowledgments

We would like to thank Mike Saks for useful conversations concerning this research and Kevin McCurley for comments on an earlier draft of this paper.

References

[1] J. C. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions.* to appear in Advances in Cryptology - CRYPTO88.

[2] G. R. Blakley, *Safeguarding cryptographic keys*, in Proceedings AFIPS 1979 National Computer Conference, vol. 48, 1979, pp. 313–317.

[3] E. F. BRICKELL, *Some ideal secret sharing schemes.* to appear in the Journal of Combinatorial Mathematics and Combinatorial Computing.

[4] M. ITO, A. SAITO, AND T. NISHIZEKI, *Secret sharing scheme realizing general access structure*, in Proceedings IEEE Globecom'87, Tokyo, Japan, 1987, pp. 99–102.

[5] A. SHAMIR, *How to share a secret*, Communications of the ACM, 22 (1979), pp. 612–613.

[6] G. J. SIMMONS, *Robust shared secret schemes.* to appear in Congressus Numerantium, Vol. 68-69.

[7] S. VAJDA, *Patterns and Configurations in Finite Spaces*, Hafner Publishing, New York, 1967.

[8] D. J. A. WELSH, *Matroid Theory*, Academic Press, London, 1976.

[9] A. YAO. Presentation at the Cryptography conference in Oberwolfach, West Germany, Sep. 1989.