J. Cryptology (1992) 5: 185–191

Journal of Cryptology

Strongly Ideal Secret Sharing Schemes

Steven J. Phillips
Computer Science Department, Stanford, CA 94305, U.S.A.

Nicholas C. Phillips
Computer Science Department, Southern Illinois University, Carbondale, IL 62901, U.S.A.

Communicated by Ernest F. Brickell

Date received 1 June 1990 and revised 30 May 1991

Abstract. We define strongly ideal secret sharing schemes to be ideal secret sharing schemes in which certain natural requirements are placed on the decoder. We prove an information-theoretic characterization of perfect schemes, and use it to determine which access structures can be encoded by strongly ideal schemes. We also discuss a hierarchy of secret sharing schemes that are more powerful than strongly ideal schemes.

Key words. Secret sharing, Ideal schemes, Access structures, Perfect security.

1. Introduction

A secret sharing scheme is a mechanism for sharing a secret among a group of people, so that only certain subgroups of people (given by an access structure) can see the secret when they pool their shares. Simmons [6] gives a comprehensive review of secret sharing schemes and their terminology. We consider only *perfect* schemes, in which a group of participants not in the access structure can gain no information about the secret by pooling their shares. Shamir [5] used the theory of polynomials over finite fields to construct efficient *threshold schemes*, in which any k people can see the secret, and no $k-1$ people can learn anything about the secret. Ito *et al.* [4] and Benaloh and Leichter [1] have given constructions for secret sharing schemes that realize arbitrary access structures.

A question that remains is to characterize access structures that can be realized by *ideal* secret sharing schemes, first defined by Brickell [2], in which the size of the share given to each participant is equal to the size of the secret. Shamir's threshold schemes are ideal. Brickell and Davenport [3] showed a correspondence between ideal secret sharing schemes and matroids.

In an ideal secret sharing scheme, the decoding mechanism can access not only the share given to the participants, but also the identity of the participants. We consider a subclass of ideal schemes, called *strongly ideal secret sharing schemes*, in

which the decoding mechanism relies only on the shares, not on the identity of the participants. The definition is formalized in the next section. These schemes have the pleasing property that when two participants swap their shares, they exchange their roles in the access structure. This property does not hold for all ideal schemes.

The main result of this paper is to show that strongly idea schemes can realize only a small class of access structures. We also describe a hierarchy of schemes with greater power than strongly ideal schemes.

2. Definitions

We take an information-theoretic perspective, rather than a computational one. In particular, we do not rely on the concept of computational intractability for the security of any secret sharing scheme.

secret A number s with $0 \leq s < n$ for some fixed integer n. The size of the secret is $\lceil \lg n \rceil$.

participant (also referred to as a *person*) A number in the range $1 \cdots k$. The set $\{1, \ldots, k\}$ of participants is denoted by P.

access structure (denoted $\mathscr{A}$) A superset-closed collection of nonempty subsets of P.

basis The basis for an access structure $\mathscr{A}$ is the smallest subset of $\mathscr{A}$ whose superset closure is the whole of $\mathscr{A}$.

bystander A person who is excluded from every set in the basis.

secret sharing scheme (also called an SSS or a sharing scheme) A pair $(\mathscr{D}, f)$ for allocating and decoding shares for a given access structure $\mathscr{A}$. Share allocation is achieved by a distribution function $\mathscr{D}$ such that $\mathscr{D}(s, r) \in \mathbf{N}^k$. Thus the ith component $\mathscr{D}(s, r)_i$ of $\mathscr{D}(s, r)$ is the share of the secret s which is distributed to person i when the distribution function is given a random string r. For a set of participants G, define $\mathscr{D}(s, r)_G$ to be the bag[1] of shares $\mathscr{D}(s, r)_i$ for all $i \in G$. The decoder is a function f mapping bags of integers to integers, such that if $G = \{i_1, \ldots, i_m\} \in \mathscr{A}$, then for each random string r and for each secret s,

$$f(\mathscr{D}(s, r)_G) = s.$$

The secret sharing scheme is said to be *perfect* if its distribution function has the property that if $G = \{i_1, \ldots, i_m\} \notin \mathscr{A}$, then, for all bags $[a_{i_1} \cdots a_{i_m}]$, $\Pr(\mathscr{D}(S, R)_G = [a_{i_1}, \ldots, a_{i_m}] | S = s)$ is the same for all secrets s. Here, and in the following, R is a random variable drawn from the uniform distribution on random strings, and S is a random variable drawn from any distribution on secrets. Lowercase letters s and r represent specific values of the random variables.

share size The share size of a sharing scheme is $\max\lceil \lg D(s, r)_i \rceil$ over all s, r, and i.

strongly ideal secret sharing scheme A perfect secret sharing scheme in which the set of possible shares is just the set of secrets. In particular, if we consider

[1] A bag, also called a multiset, is a set that can have repeated elements. Bags are appropriate since the distribution function may allocate the same share to several people. We use square brackets [ ] to denote bags and braces { } to denote sets.

secrets s satisfying $0 \leq s < n$ where n is a power of 2, this definition is equivalent to the share size and secret size being equal.

The definition of *perfect* given above suggests informally that a perfect scheme is one in which any set of participants not in the access structure cannot extract any information about the secret from their shares. We formalize this characterization of perfect schemes, and prove it equivalent to the original definition. We then derive a useful test for nonperfectness that we use in later proofs.

Lemma 1. *Let the secret sharing scheme $(\mathscr{D}, f)$ be perfect. For any probability distribution on the set of secrets, if G is not in the access structure and the bag B can be distributed to G, then $\Pr(S = s | \mathscr{D}(S, R)_G = B) = \Pr(S = s)$ for all secrets s. In other words, the random variables S and $\mathscr{D}(S, R)_G$ are independent. Conversely, if the last statement holds for some probability distribution that assigns nonzero probabillty to each secret, then the secret sharing scheme is perfect.*

Proof. For any set G of participants, any secret s and any bag B that can be distributed to G,

$$\begin{aligned}\Pr(\mathscr{D}(S, R)_G = B | S = s) \times \Pr(S = s) \\ = \Pr(\mathscr{D}(S, R)_G = B \text{ and } S = s) \\ = \Pr(S = s | \mathscr{D}(S, R)_G = B) \times \Pr(\mathscr{D}(S, R)_G = B).\end{aligned}$$

If the scheme is perfect and $G \notin \mathscr{A}$, then from the first and third lines above, $\Pr(S = s | \mathscr{D}(S, R)_G = B)$ and $\Pr(S = s)$ can differ only by a factor that is independent of s—in fact this factor must be 1 as can be seen by summing over all s.

Conversely, if for some probability distribution on secrets, we have

$$\Pr(S = s | \mathscr{D}(S, R)_G = B) = \Pr(S = s) \neq 0$$

for each secret s, each $G \notin \mathscr{A}$, and each bag B that can be distributed to G, then from the first and third lines above, $\Pr(\mathscr{D}(s, R)_G = B)$ is the same for all s, so the scheme is perfect. □

Lemma 2. *A secret sharing scheme is perfect iff it has the following property: if $G = \{i_1, \ldots, i_m\} \notin \mathscr{A}$, then, for any randomized or deterministic function g with range contained in $0 \cdots n - 1$, $\Pr(g(\mathscr{D}(S, R)_G) = S) = 1/n$, where the probability is over independent and uniform choices of R, S, and any random bits R' used by g.*

Proof. If g is randomized and $\Pr(g(\mathscr{D}(S, R)_G) = S) > 1/n$, then there is a setting of g's random bits that preserves the inequality. In other words, if $g_{r'}$ is the function g with random bits r', then there is an assignment to r' such that $\Pr(g_{r'}(\mathscr{D}(S, R)_G) = S) > 1/n$, so we can assume from here on that g is deterministic.

If we invoke Lemma 1 with the uniform distribution on secrets, we have that the scheme is perfect iff for all G not in the access structure and for all B that can be distributed to G, $\Pr(S = s | \mathscr{D}(S, R)_G = B) = 1/n$ for each secret s.

Finally,

$$\Pr(S = s | \mathscr{D}(S, R)_G = B) = 1/n \quad \text{for all } s \text{ and } B \tag{1}$$

$$\Leftrightarrow \quad \Pr(g(\mathscr{D}(S, R)_G) = S) = 1/n \quad \text{for all } g \text{ with range contained in } 0 \cdots n - 1. \tag{2}$$

(1) $\Rightarrow$ (2) follows from

$$\begin{aligned}\Pr(g(\mathscr{D}(S, R)_G) = S) &= \sum_B \Pr(g(\mathscr{D}(S, R)_G) = S \text{ and } \mathscr{D}(S, R)_G = B) \\ &= \sum_B \Pr(g(\mathscr{D}(S, R)_G) = S | \mathscr{D}(S, R)_G = B) \times \Pr(\mathscr{D}(S, R)_G = B) \\ &= \sum_B \frac{1}{n} \times \Pr(\mathscr{D}(S, R)_G = B) \qquad \text{if (1) holds.}\end{aligned}$$

To see (2) $\Rightarrow$ (1), assume that the bag B' and the secret s' satisfy

$$\Pr(S = s' | \mathscr{D}(S, R)_G = B') > 1/n.$$

Define a function g, by $g(B') = s'$, and for any bag $B \neq B'$, let $g(B)$ be a secret s satisfying $\Pr(S = s | \mathscr{D}(S, R)_G = B) \geq 1/n$. Then $\Pr(g(\mathscr{D}(S, R)_G) = S) > 1/n$. □

The above definition of a secret sharing scheme is a strong one. It provides complete information-theoretic security. It does not rely on keeping the distribution and decoding functions and the access structure hidden. Some additional security might be obtained by keeping one or more of these secret or by using identity checks, but that is outside the present notion of a secret sharing scheme. The people sharing a secret need not prove their identity, since the decoder uses only their share values. In particular, if two people swap their shares, their roles in the access structure are also swapped. Participants need to know only their own role in the access structure, namely who they need with them to see the secret, to use the scheme.

3. Access Structures with Strongly Ideal Sharing Schemes

We study strongly ideal secret sharing schemes, in which the set of possible shares is just the set of secrets. It turns out that the number of access structures with strongly ideal sharing schemes depends heavily on the details in the definition of a secret sharing scheme. We first show that very few access structures have strongly ideal sharing schemes. We then show that easing the requirements on the decoder greatly increases the number of access structures that can be realized.

3.1. *Characterizing Strongly Ideal Sharing Schemes*

Lemma 3. *If $(\mathscr{D}, f)$ is a strongly ideal sharing scheme for an access structure with a basis set B, then the range of $\mathscr{D}$ projected onto the set B is $\{0 \cdots n-1\}^{|B|}$.*

Proof. Each share is in the range $0 \cdots n-1$, as the sharing scheme is strongly ideal. Now assume that the distribution function has given shares to everyone in B except person i. If i cannot be given some share in the range $0 \cdots n-1$ while the rest of the shares in B remain fixed, then the people in $B \backslash \{i\}$ can conspire to guess the secret by choosing a share for i that *can* be given by the distribution function, and give this guess and their own shares to the decoder. Their guess has probability at least $1/(n-1)$ of being correct, so by Lemma 2, the scheme is not perfect.

Thus starting from a vector of shares for B we can change each person's share,

one by one, till the shares are any vector in $\{0 \cdots n-1\}^{|B|}$, while remaining in the image of the distribution function. □

Theorem 1. *An access structure has a strongly ideal sharing scheme if and only if its basis is of one of the following types*:

1. $\{X\}$ *for some* $X \subseteq P$.
2. $\{\{x\}: x \in X\}$ *for some* $X \subseteq P$.
3. $\{\{x, y\}: x \in X, y \in Y\}$ *for disjoint subsets* X *and* Y *of* P.

Proof. Let $\mathscr{B}$ be the basis for an access structure $\mathscr{A}$, and let $(\mathscr{D}, f)$ be a strongly ideal sharing scheme for $\mathscr{A}$, in other words, the set of possible shares is just the set $\{0, \cdots n-1\}$ of secrets.

Let C and D be distinct basic sets: there must be c and d in $C \backslash D$ and $D \backslash C$ respectively, since $\mathscr{B}$ is a basis. Let $F = C \cup D \backslash \{c\} \backslash \{d\}$. $\mathscr{A}$ must contain both $F \cup \{c\}$ and $F \cup \{d\}$, since the first is a superset of C and the second is a superset of D. We now have one of two cases.

1. $F \in \mathscr{A}$, so there is an $E \in \mathscr{B}$ such that $E \subseteq F$. In this case there must be $e \in E \backslash C$, and we can repeat the argument above with E in the place of D. Since $|E \backslash C| < |D \backslash C|$ we must eventually get:
2. $F \notin \mathscr{A}$. Both $F \cup \{c\}$ and $F \cup \{d\}$ are in $\mathscr{A}$, and since the secret sharing scheme is perfect, applying Lemma 2 gives us that d's share uniquely determines the value of f on the shares of $F \cup \{d\}$, and the share of c uniquely determines the value of f on the shares of $F \cup \{c\}$. By assumption there are exactly as many possible values for c and d as for the secret s, so we must have that c and d receive the same shares. Since this is true for any value of the random variable r used by the share distribution function, and the sharing scheme is perfect, c and d must be equivalent in $\mathscr{A}$, in the sense that any occurrence of c could be replaced by d, and vice versa. Hence we can consider a reduced access structure in which the roles of c and d are combined, by replacing all occurrences of d by c.

We can continue shrinking the access structure until we reach an access structure $\mathscr{A}'$ that has the basis $\mathscr{B}'$ with only one element, say $\{1, \ldots, t\}$. Consider the previous access structure $\mathscr{A}''$ involving one more person $t+1$: $t+1$ must have been combined with some person, say t. $\mathscr{A}''$ must therefore have the basis $\{\{1, \ldots, t\}, \{1, \ldots, t-1, t+1\}\}$. We wish to show that $t \leq 2$. First we require some notation: let us use a subscript to denote the owner of a share. As an example, x_i means "the number x, which is the share that was given to person i."

Assume that $t > 2$: then we have $f([1_1, 1_2, 0_3, \ldots, 0_t, 0_{t+1}])$ (middle arguments all 0) is always $f([0_1, 0_2, \ldots, 0_{t-1} 1_t, 1_{t+1}])$ since the bags are identical and in the range of the distribution function (by Lemma 3, and since t and $t+1$ are equivalent). Therefore $f([0_1, 0_2, \ldots, 0_{t-1} 1_t]) = f([1_1, 1_2, 0_3, \ldots, 0_t])$ since $\{1, \ldots, t\} \in \mathscr{B}$; reordering shares in the bag gives us

$$f([0_1, 1_2, 0_3, \ldots, 0_{t-1}, 0_t]) = f([0_1, 1_2, 0_3, \ldots, 0_{t-1}, 1_t]).$$

Put in words, when persons 1 and 2 are given the shares 0 and 1, the secret is the same whether person t is given share 0 or 1. Therefore when persons 1

and 2 are given these values, they can (in combination with persons $3 \cdots t-1$) guess the secret correctly with probability at least $1/(n-1)$, so by Lemma 2 the scheme is not perfect. Hence we must have $t \leq 2$.

Thus the original access structure $\mathscr{A}$ falls into one of three categories:

1. No shrinking is possible, as $\mathscr{B} = \{X\}$ for some $X \subseteq P$. $\mathscr{A}$ has the following strongly ideal sharing scheme: the bystanders are given a fixed value, say 0. All but one element of X is given a random value, the last is given the x-or of the others with the secret. Decoding is done by the x-or of the bag of shares. The bystanders' zero shares do not affect the value of the x-or.
2. $t = 1$ and shrinking is possible. The access structure $\mathscr{A}$ has the basis $\{\{x\}: x \in X\}$ for some $X \subseteq P$. This access structure has a strongly ideal sharing scheme: give each bystander the share 0, and give each $x \in X$ the secret. The decoder returns any nonzero share, or zero if each share given to it is zero.
3. $t = 2$ and shrinking is possible. $\mathscr{A}$ must have the basis

$$\{\{x, y\}: x \in X, y \in Y\}$$

for disjoint subsets X and Y of P. A strongly ideal sharing scheme for this access structure gives 0 to each bystander, the same random value to each $x \in X$, and the x-or of the random value and the secret to each member of Y. The decoder returns 0 if all shares given to it are the same, otherwise it returns the x-or of the two largest distinct share values given to it. □

The theorem can be more simply stated if the access structure has no bystanders. In this case, there is a strongly ideal sharing scheme iff the access structure has one of the following bases:

1. $\{P\}$,
2. $\{\{x\}: x \in P\}$,
3. $\{\{x, y\}: x \in X, y \in Y\}$ for some partition (X, Y) of P.

3.2. *Relaxing the Definitions*

The characterization given in the last section depends heavily on the fine details in the definitions associated with secret sharing schemes. We describe how relaxing the definitions slightly would allow many more access structures to have strongly ideal sharing schemes.

3.2.1. *A Hierarchy of Almost Strongly Ideal Sharing Schemes.* The strictness of the definition of strong ideality is crucial to the characterization given in Section 3.1. If we allow each share to contain m extra bits, then we can easily get sharing schemes for access structures with bases of the form $X_1 \times X_2 \times \cdots \times X_{2^m}$ for disjoint sets X_i, by giving each share a "group identifier." In particular, if each share has $\lg k$ extra bits, where k is the number of participants, then we can realize any access structure realizable by a sharing scheme which is ideal in the sense of [3].

3.2.2. *Correctness only on a Basis.* Since participants in a secret sharing scheme should know with whom they need to collaborate to learn the secret, it is reasonable

to ask that the decoder only be correct when given the shares of a group of people in the basis. In this case the number of access structures with strongly ideal sharing schemes is much greater. For example, any access structure with a basis of disjoint sets will have a strongly ideal sharing scheme that is correct only on the basis.

Acknowledgments

We would like to thank Robert Kennedy, Rajeev Motwani, Walter Wallis, and E. F. Brickell for helpful suggestions.

References

[1] J. C. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Advances in Cryptology—Crypto '88 Proceedings*, Springer-Verlag, Berlin, 1988, pp. 27–35.

[2] E. F. Brickell, Some ideal secret sharing schemes, *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 6 (1989), pp. 105–113.

[3] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *Advances in Cryptology—Crypto '89 Proceedings*, Springer-Verlag, Berlin, 1989, pp. 278–285.

[4] M. Ito, A. Saito, and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proceedings of the IEEE Global Telecommunications Conference Globecom '87*, Tokyo, IEEE Communications Society Press, Washington, DC, 1987, pp. 99–102.

[5] A. Shamir, How to share a secret, *Communications of the ACM* vol. 22 (1979), no. 11, pp. 612–613.

[6] G. Simmons, An introduction to shared secret and/or shared control schemes and their applications, in *Contemporary Cryptology: the Science of Information* (ed. G. J. Simmons), IEEE Press, New York, 1992.