J. Cryptology (1997) 10: 223–231

Journal of
CRYPTOLOGY

The Size of a Share Must Be Large*

László Csirmaz
Mathematical Institute of the Hungarian Academy of Sciences,
Reáltanoda u. 13-15, Budapest, Hungary H-1053

Communicated by Ernest F. Brickell

Received 24 November 1993 and revised 15 September 1995

Abstract. A secret sharing scheme permits a secret to be shared among participants of an n-element group in such a way that only qualified subsets of participants can recover the secret. If any nonqualified subset has absolutely no information on the secret, then the scheme is called *perfect*. The *share* in a scheme is the information that a participant must remember.

In [3] it was proved that for a certain access structure any perfect secret sharing scheme must give some participant a share which is at least 50% larger than the secret size. We prove that for each n there exists an access structure on n participants so that any perfect sharing scheme must give some participant a share which is at least about $n/\log n$ times the secret size.[1] We also show that the best possible result achievable by the information-theoretic method used here is n times the secret size.

Key words. Secret sharing, Ideal secret sharing schemes, Polymatroid structures, Perfect security.

1. Introduction

An important issue in secret sharing schemes is the size of the shares distributed to the participants, since the security of a system degrades if the amount of the information that must be kept secret increases. The problem of giving bounds on the size of the secret some participant must have has received considerable attention in the last few years, see, e.g., [10], [3], and [4].

Capocelli *et al*. [3] showed that in a certain access structure with four participants the number of the bits some participant must remember is at least 1.5 times the number of bits in the secret. They generalized the construction to any number of participants with the same bound. Their method was information-theoretic, namely, the results were followed by a close examination of the *entropy* of the information a group of the participants have. The connection between the entropy and matroid-theory was observed by Fujishige [7],

* This research was supported by OTKA Grant no. 1911.
[1] All logarithms in this paper are of base 2.

and in the context of a secret sharing scheme by Brickell and Davenport [2] and by Kurosawa *et al*. [9]. Here we expand these ideas to our main result:

Theorem 1.1. *For each n there exists an access structure $\mathcal{A}$ on n participants so that any perfect secret sharing scheme assigns a share of length about $n/\log n$ times the length of the secret to some participant.*

We give a construction which shows that apart from the $\log n$ factor, our result is the best possible. That is, the information-theoretic method cannot yield a lower bound for the size of the share of the participants better than n times the size of the secret.

We call a participant x *unimportant* if no unqualified group becomes qualified by adapting x. Obviously, in any secret sharing scheme the share of an unimportant participant can be safely disregarded, thus x's share can be considered zero. The following theorem is implicit in [3]:

Theorem 1.2. *In any perfect secret sharing scheme, all important participants must have a share at least as large as the secret itself.*

This bound is the best possible, as Capocelli *et al*. [3] observed that in any access structure fixing any participant x, it is possible to distribute the shares so that x's share will be of the same length as the secret.

2. Preliminaries

In this section we review the technical concepts as well as some earlier results. For a complete treatment of information theory the reader is referred to [6]; its application to secret sharing is explained in details in [3]. For the sake of completeness we repeat here some definitions and lemmas.

2.1. *Information-Theoretic Notions*

Given a probability distribution $\{p(x)\}_{x\in X}$ on a finite set X, define the *entropy* of X, $H(X)$, as

$$H(X) = -\sum_{x\in X} p(x)\log p(x).$$

The entropy $H(X)$ is a measure of the average information content of the elements in X. It is well known that $H(X)$ is a good approximation to the average number of bits needed to represent the elements of X faithfully. By definition, the entropy is always nonnegative.

Given two sets X and Y and a joint probability distribution $\{p(x,y)\}_{x\in X, y\in Y}$ on the Cartesian product of X and Y, the *conditional entropy* $H(X|Y)$ of X assuming Y is defined as

$$H(X|Y) = \sum_{y\in Y} p(y) H(X|Y=y), \tag{1}$$

where "$X|Y = y$" is the probability distribution derived from p by fixing the value $y \in Y$. The conditional entropy can also given in the form

$$H(X|Y) = H(XY) - H(Y), \tag{2}$$

where Y is the marginal distribution. From definition (1) it is easy to see that $H(X|Y) \geq 0$.

The *mutual information* between X and Y is defined by

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) = H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(XY) \end{aligned}$$

and is always nonnegative: $I(X;Y) \geq 0$. This inequality expresses the intuitive fact that the knowledge of Y, on average, can only decrease the uncertainty one has on X.

Similarly to the conditional entropy, the *conditional mutual information* between X and Y given Z is defined as

$$\begin{aligned} I(X;Y|Z) &= H(X|Z) - H(X|YZ) \\ &= H(XZ) + H(YZ) - H(XYZ) - H(Z), \end{aligned} \tag{3}$$

and is also nonnegative: $I(X;Y|Z) \geq 0$.

2.2. *Secret Sharing Schemes*

In the following, individuals are denoted by small letters, a, b, x, y, etc., sets (groups) of individuals by capital letters, A, B, X, Y, etc., and finally collections of groups by script letters, $\mathcal{A}, \mathcal{B}$. We use P to denote the set of *participants* who will share the secret.

An *access structure* on an n-element set P of participants is a collection $\mathcal{A}$ of subsets of P: only exactly the qualified groups are collected into $\mathcal{A}$. We denote a group simply by listing its members, so x denotes both a member of P and the group which consists solely of x. It will always be clear from the context which meaning we are using.

A secret sharing scheme permits a secret to be shared among n participants in such a way that only qualified subsets of them can recover the secret. Secret sharing schemes satisfying the additional property that unqualified subsets can gain absolutely no information about the secret are called *perfect* as opposed to schemes where unqualified groups may obtain some information on the secret (e.g., the ramp schemes in [1]).

A natural property of the access structures is its *monotonicity*, i.e., $A \in \mathcal{A}$ and $A \subseteq B \subseteq P$ implies $B \in \mathcal{A}$. This property expresses the fact that if any subset of B can recover the secret, then the participants in B can also recover the secret. Also, a natural requirement is that the empty set should not be in $\mathcal{A}$, i.e., there must be some secret. Access systems of this type are called *Sperner systems*, named after E. Sperner who was first to determine the maximal number of subsets in such a system [11].

Let P be the set of participants, let $\mathcal{A}$ be a Sperner system on P, and let S be the set of secrets. A *secret sharing scheme*, given a secret s, assigns to each member $x \in P$ a random *share* from some domain. The shares are thus random variables with some joint distribution determined by the value of the secret $s \in S$. Thus a scheme can be regarded as a collection of random variables, one for the secret and one for each $x \in P$. The scheme determines the joint distribution of these $n + 1$ random variables. For $x \in P$,

x's share, which is (the value of) a random variable, is denoted by x. For a subset A of participants, A also denotes the joint (marginal) distribution of the shares assigned to the participants in A.

Following [3] we call the scheme *perfect* if the following hold:

1. Any qualified subset can reconstruct the secret, that is, the shares of the participants in A uniquely determine the secret. This means $H(s|A) = 0$ for all $A \in \mathcal{A}$.
2. Any nonqualified subset has absolutely no information on the secret, i.e., s and the shares of members of A are statistically independent: knowing the shares in A, the conditional distribution of s is exactly the same as its *a priori* distribution. Translated to information-theoretic notions this gives $H(s|A) = H(s)$ for all $A \notin \mathcal{A}$.

By the above discussion the entropy of the secret, $H(s)$, can be considered as the *length* of the secret. Any lower bound on the entropy of $x \in P$ immediately gives a lower bound on the size of x's share: if $H(x) \geq \lambda H(s)$, then x's share is at least λ times the size of the secret.

2.3. *Polymatroid Structure*

Let Q be any finite set, and let $\mathcal{B} = 2^Q$ be the collection of the subsets of Q. Let $f: \mathcal{B} \to \mathbf{R}$ be a function assigning real numbers to subsets of Q and suppose f satisfies the following conditions:

(i) $f(A) \geq 0$ for all $A \subseteq Q$, $f(\emptyset) = 0$,
(ii) f is monotone, i.e., if $A \subseteq B \subseteq Q$, then $f(A) \leq f(B)$,
(iii) f is submodular, i.e., if A and B are different subsets of Q, then $f(A) + f(B) \geq f(A \cap B) + f(A \cup B)$.

The system (Q, f) is called *polymatroid*. If, in addition, f takes only integer values and $f(x) \leq 1$ for one-element subsets, then the system is a *matroid*.

Fujishige in [7] observed that having a finite collection of random variables, we will get a polymatroid by assigning the entropy to each subset.

Proposition 2.1. *By defining $f(A) = H(A)/H(s)$ for each $A \subseteq P \cup \{s\}$ we get a polymatroid.*

Proof. We check (i)–(iii) of the definition of the polymatroid. (i) is immediate since the entropy is always nonnegative. (ii) follows from (2) by letting $X = B$, $Y = A$. Then $XY = X \cup Y = X$, i.e.,

$$f(B) - f(A) = H(XY) - H(Y) = H(X|Y) \geq 0.$$

Similarly, (iii) follows easily from (3) and from the fact that the conditional mutual information $I(X; Y|Z) \geq 0$. $\square$

Unfortunately, it is not known whether the converse of this proposition holds, i.e., all polymatroids over a finite set can be obtained as the entropy of appropriately chosen random variables [5]. We elaborate on this later.

In our case the random variable s, the "secret," plays a special role. By our extra assumption on the conditional entropies containing s, we can calculate the value of $f(As)$ from $f(A)$ for any $A \subseteq P$.

Proposition 2.2. *If the secret sharing scheme is perfect, then for any $A \subseteq P$ we have*

if $A \in \mathcal{A}$, then $f(As) = f(A)$;
if $A \notin \mathcal{A}$, then $f(As) = f(A) + 1$.

Proof. If $A \in \mathcal{A}$, then A is a qualified subset, and thus $H(s|A) = 0$. By definition, $H(s|A) = H(sA) - H(A)$, and the first claim follows.

If $A \notin \mathcal{A}$, then A is an unqualified subset, and then $H(s|A) = H(s)$, which yields the second claim. □

Now we consider the function f defined in Proposition 2.1 restricted to the subsets of P. From this restriction we can easily calculate the whole function; and since the extension is also a polymatroid, the restriction will satisfy some additional inequalities.

Proposition 2.3. *The function f defined in Proposition* 2.1 *satisfies the following additional inequalities*:

(i) *if $A \subseteq B$, $A \notin \mathcal{A}$, and $B \in \mathcal{A}$, then $f(B) \geq f(A) + 1$;*
(ii) *if $A \in \mathcal{A}$, $B \in \mathcal{A}$, but $A \cap B \notin \mathcal{A}$, then $f(A) + f(B) \geq f(A \cap B) + f(A \cup B) + 1$.*

Proof. If $A \subseteq B$, then $As \subseteq Bs$, therefore by the monotonicity of f we have

$$f(A) + 1 = f(As) \leq f(Bs) = f(B),$$

which gives (i). Similarly, using the submodularity for the sets As, Bs we get (ii). □

The claim of this proposition can be reversed: given any polymatroid f on the subsets of P satisfying (i) and (ii) above and extending f to the subsets of $P \cup \{s\}$ as defined in Proposition 2.2, we get a polymatroid.

3. Results

We start by proving

Theorem 3.1. *In any perfect secret sharing scheme, all important participant must have a share at least as large as the secret itself.*

Proof. Suppose an access structure $\mathcal{A}$ is given on the set P of participants, $x \in P$ is an important person shown by $C \subseteq P$, i.e., $C \notin \mathcal{A}$ but $Cx \in \mathcal{A}$. Also given any perfect secret sharing scheme, consider the function f defined in Proposition 2.1. Since $f(x) = H(x)/H(s)$, $f(x) \geq 1$ implies $H(x) \geq H(s)$, i.e., that the (average) size of x's share must be at least as large as the (average) size of the secret. Thus we have to show only that $f(x) \geq 1$.

Since $C \notin \mathcal{A}$ and $Cx \in \mathcal{A}$, by Proposition 2.3(i) we have $f(Cx) \geq f(C) + 1$. f is submodular on the subsets of P, so we also have

$$f(C) + f(x) \geq f(Cx) + f(C \cap \{x\}) = f(Cx) + f(\emptyset) = f(Cx)$$

since $x \notin C$. Combining this with $f(Cx) \geq f(C) + 1$ we get the desired result. □

Theorem 3.2. *For each n there exists an access structure $\mathcal{A}$ on n participants so that any perfect secret sharing scheme assigns a share of length about $n/\log n$ times the length of the secret to some participant.*

Proof. Suppose an access structure $\mathcal{A}$, to be defined later, is given on the n-element set P of participants. Let k be the largest integer with $2^k + k - 2 \leq n$. Suppose also that a perfect secret sharing scheme is given, and consider again the function f defined in Proposition 2.1. We have to find a participant $x \in P$ such that $f(x)$ is at least $(2^k - 1)/k$ which is approximately equal to $n/\log n$ (for example, it is always between $n/2\log n$ and $n/\log n$).

We illustrate the construction by an example for $k = 2$. Let a, b, c, d be different members of P. (Since $2^k + k - 2 = 4 \leq n$, there are at least four members in P.) Let the sets ab, ca, and cdb be minimal sets in the Sperner system $\mathcal{A}$, i.e., none of their proper subsets is in $\mathcal{A}$ (see Fig. 1, elements of $\mathcal{A}$ are denoted by solid dots).

Now consider the following differences:

(i) $f(cdab) - f(cd)$;
(ii) $f(cab) - f(c)$;
(iii) $f(ab) - f(\emptyset)$.

Since $cdab \in \mathcal{A}$ and $cd \notin \mathcal{A}$, by Proposition 2.3(i) we have (i) ≥ 1. We claim that each difference is at least 1 larger than the previous one. To show this, we use Proposition 2.3(ii) and the submodularity of f as follows. Since cdb and cab are both in $\mathcal{A}$, but their intersection $cb \notin \mathcal{A}$, we have

$$f(cdb) + f(cab) \geq f(cdab) + f(cb) + 1.$$

Applying the submodularity to cd and cb we have

$$f(cd) + f(cb) \geq f(cdb) + f(c).$$

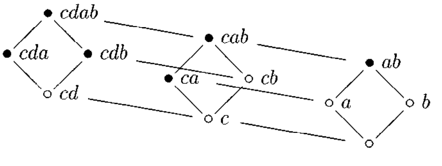

Fig. 1. The case $k = 2$.

Adding and rearranging the terms we get

$$f(cab) - f(c) \geq f(cdab) - f(cd) + 1,$$

which shows that (ii) $\geq$ (i) $+ 1$.

Similarly, applying Proposition 2.3(ii) to ca and ab and the submodularity to c and a we get (iii) $\geq$ (ii)$+1 \geq$ (i)$+2 \geq 3$. Now since $f(a)+f(b) \geq f(ab)$ (by submodularity again), which is ≥ 3, either $f(a)$ or $f(b)$ must be at least 1.5, i.e., either a or b must have a share with size 50% bigger than the size of the secret. This was the main result in [3] using a slightly different access structure.

Now we turn to the general construction. Let A be a k-element set of individuals, and let $A = A_0, A_1, \dots, A_{2^k-1} = \emptyset$ be a decreasing enumeration of all of its subsets so that if $i < j$, then $A_i \not\subseteq A_j$. Let $B = \{b_1, b_2, \dots, b_{2^k-2}\}$ be disjoint from A, our set of individuals will be $A \cup B$. Since $k + 2^k - 2 \leq n$ we can pick A and B from P. Let $B_0 = \emptyset$, and in general $B_i = \{b_1, b_2, \dots, b_i\}$. The minimal elements of the access structure $\mathcal{A}$ will be $U_i = A_i \cup B_i$ for $i = 0, 1, \dots, 2^k - 2$. They are pairwise incomparable, i.e., none of them is a subset of the other; this means that they can indeed form the minimal elements in an access structure. To check it, let $i < j$, then $b_j \in U_j - U_i$ (i.e., $U_j \not\subseteq U_i$), and $\emptyset \neq A_i - A_j \subseteq U_i - U_j$ (i.e., $U_i \not\subseteq U_j$).

Lemma 3.3. *Under these assumptions, for each* $0 \leq i < 2^k - 2$,

$$[f(B_i \cup A) - f(B_i)] - [f(B_{i+1} \cup A) - f(B_{i+1})] \geq 1.$$

Proof. Just mimic the proof for the case $k = 2$. Choosing $X = B_i \cup A$, $Y = B_{i+1} \cup A_{i+1}$, both of them are in $\mathcal{A}$ since $X \supseteq U_i$, and $Y = U_{i+1}$, while $X \cap Y = B_i \cup A_{i+1} \notin \mathcal{A}$. To see this it is enough to check that, for all j, $U_j = A_j \cup B_j \not\subseteq B_i \cup A_{i+1}$. Indeed, if $j \leq i$, then $A_j \not\subseteq A_{i+1}$; if $j > i$, then $B_j \not\subseteq B_i$. Therefore by Proposition 2.3(ii) we have

$$f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y) + 1,$$

or, by rearranging,

$$[f(B_i \cup A) - f(B_i \cup A_{i+1})] - [f(B_{i+1} \cup A) - f(B_{i+1} \cup A_{i+1})] \geq 1. \tag{4}$$

The submodularity of f applied to $X = B_i \cup A_{i+1}$ and $Y = B_{i+1}$ gives

$$f(X) + f(Y) \geq f(X \cup Y) + f(X \cap Y),$$

i.e., also by rearranging the terms

$$[f(B_i \cup A_{i+1}) - f(B_i)] - [f(B_{i+1} \cup A_{i+1}) - f(B_{i+1})] \geq 0. \tag{5}$$

By adding inequalities (4) and (5) we get the claim of the lemma. □

Lemma 3.4. $f(A) \geq 2^k - 1$.

Proof. Note that $f(A \cup B_{2^k-2}) - f(B_{2^k-2}) \geq 1$ by Proposition 2.3(i) since $A \in \mathcal{A}$ but $B_{2^k-2} \notin \mathcal{A}$. Now adding this to the inequality in Lemma 3.3 for all $0 \leq i < 2^k - 2$ we get

$$f(B_0 \cup A) - f(B_0) \geq 2^k - 1,$$

which, by $B_0 = \emptyset$, gives the result. □

Finally, by iterated application of the submodularity inequality,

$$f(a_1) + f(a_2) + \cdots + f(a_k) \geq f(A),$$

thus at least one of $f(a_i) \geq (2^k - 1)/k$, which was to be proven. □

We show that apart from the $\log n$ factor, our result is the best possible. Namely, the method cannot give a better lower bound than n times the length of the secret.

Theorem 3.5. *Given any access structure $\mathcal{A}$ on the n-element set P, we can always find a polymatroid function f so that*

(i) *f satisfies the conditions of Proposition* 2.3;
(ii) *$f(x) \leq n$ for all elements $x \in P$.*

Proof. Let A be a k-element subset of P, define

$$f(A) = n + (n-1) + \cdots + (n+1-k).$$

This function assigns n to each one-element set. If A is a proper subset of B, then $f(B) - f(A)$ is the sum of $|B - A|$ consecutive positive integers, therefore it is ≥ 1, and equality holds only if $B = P$ and A is an $(n-1)$-element subset. This proves (i) of Proposition 2.3, and also proves the monotonicity of f. To check (ii), suppose that $A \cap B$ is a proper subset of both A and B. Observe that $(A \cup B) - A$ and $B - (A \cap B)$ is the same nonempty set, and suppose this difference contains, say, $\ell \geq 1$ elements. Then both $f(A \cup B) - f(A)$ and $f(B) - f(A \cap B)$ are the sums of ℓ consecutive integers, and since $A \cup B$ has more elements than B, each number in the first sum is bigger than the corresponding number in the second sum. Thus

$$f(A \cup B) - f(A) > f(B) - f(A \cap B),$$

and since the values are integers, the difference between the two sides is at least 1, as was required. □

4. Conclusion and Future Work

We have constructed an access structure $\mathcal{A}$ on n elements so that any perfect secret sharing scheme must assign a share which is of size at least $n/\log n$ times the size of the secret. The best previous upper bound was 1.5 [3]. From the other side, for our access structure we can construct a scheme which, for each secret bit, assigns at most n bits to each participant. This means that in this case the upper and lower bounds are quite close.

Recall that the access structure $\mathcal{A}$ is generated by the minimal subsets U_i for $i = 0, 1, \ldots, 2^k - 2$. Let s be a secret bit, and for each i pick $|U_i|$ random bits so that their mod 2 sum is equal to s. Distribute these bits among the members of U_i. Each participant gets as many bits as the U_i's he or she is in, thus each share is at most $2^k - 1 \leq n$ bits.

We have seen in Theorem 3.5 that using polymatroids we cannot prove essentially better lower bounds. For general access structures, however, the known general techniques produce exponentially large shares [8]. In order to turn the construction in Theorem 3.5 into an actual secret sharing scheme, thus proving that every access structure can be realized within an n-factor blow-up in shares, the first obstacle to be overcome is the following problem.

Problem 4.1. Can every polymatroid be represented as the entropy of appropriately chosen random variables?

An affirmative answer would help in completing the construction. However, intuition says that the answer is *no* [5], and sometimes the size of a share must be much larger. In this case we have to deal with additional inequalities the entropy function does not share with polymatroids. These might help in establishing better lower bounds for the size of the shares.

References

[1] G. R. Blakley and C. Meadows, Security of Ramp Schemes, *Proceeding of Crypto '84—Advances in Cryptology*, Lecture Notes in Computer Science, Vol. 196, G. R. Blakley and D. Chaum, eds., Springer-Verlag, Berlin, 1985, pp. 411–431.

[2] E. F. Brickell and D. M. Davenport, On the Classification of Ideal Secret Sharing Schemes, *Journal of Cryptology*, Vol. 4 (1991), pp. 123–134.

[3] R. M. Capocelli, A. De Santis, and U. Vaccaro, On the Size of Shares for Secret Sharing Schemes, *Journal of Cryptology*, Vol. 6 (1993), pp. 157–167.

[4] M. Carpentieri, A. De Santis, and U. Vaccaro, Size of Shares and Probability of Cheating in Threshold Schemes, *Proceedings of Eurocrypt '93*, Lecture Notes in Computer Science, Vol. 765, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, pp. 118–125.

[5] I. Csiszár, Personal communication.

[6] I. Csiszár and J. Körner, *Information Theory. Coding Theorems for Discrete Memoryless Systems*, Academic Press, New York, 1981.

[7] S. Fujishige, Polymatroid Dependence Structure of a Set of Random Variables, *Information and Control*, Vol. 39 (1978), pp. 55–72.

[8] M. Ito, A. Saito, and T. Nishizeki, Multiple Assignment Scheme for Sharing Secret *Journal of Cryptology*, Vol. 6 (1993), pp. 15–20.

[9] K. Kurosawa, K. Okada, K. Sakano, W. Ogata, and S. Tsujii, Nonperfect Secret Sharing Schemes and Matroids, *Proceedings of Eurocrypt '93*, Lecture Notes in Computer Science, Vol. 765, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, pp. 126–141.

[10] G. J. Simmons, An Introduction to Shared Secret and/or Shared Control Schemes and Their Application, in *Contemporary Cryptology*, IEEE Press, New York, 1991, pp. 441–497.

[11] E. Sperner, Ein Stas über Untermengen einer endlichen Menge, *Mathematische Zeitschrift*, Vol. 27 (1928), pp. 544–548.