NOT ALL PERFECT EXTRINSIC SECRET SHARING SCHEMES ARE IDEAL

W. D. WALLIS[1]

Department of Mathematics, Southern Illinois University
Carbondale, Illinois 62901-4408

Abstract. We construct a perfect extrinsic secret sharing scheme for any case in which a set of participants can gain access to the secret if and only if the set contains a pair of members from some given list of pairs.

A *secret sharing scheme* is a way by which a dealer may distribute secret information (called *shares*) to individuals (call *participants*). There is associated an *access structure* consisting of subsets of participants; a set of participants can determine the secret if and only if they constitute a member of the access structure. It is usual to demand that the access structure be *monotone*: If A contains a subset which belongs to the access structure, then A itself must also belong to the structure.

A secret sharing scheme is called *perfect* if a set of participants can gain *no* information by pooling their shares unless the set is a member of the access structure. An access structure is called *extrinsic* [3] if each participant's share contains the same amount of information. Simmons [4] has pointed out the desirability of a scheme which is perfect and the access structure of which is extrinsic. Observe that in such a scheme the amount of information in the secret will equal at most the amount of information in each share.

Brickell [2] uses a somewhat stronger concept than a perfect extrinsic structure. He asks for what he calls an *ideal* scheme, which he defines to be a perfect scheme in which the number of possible secrets is equal to the number of possible shares available to each participant. Such a scheme is clearly extrinsic.

We define a set $\sum$ of subsets of the participants to be a *basis* for the access structure Γ if Γ consists precisely of those sets of participants with a subset belonging to $\sum$. It is usually convenient to use a minimal basis, but this is not essential - we even admit Γ as a basis for itself.

We now outline a secret sharing scheme for a set P of w participants $p_1, p_2, \ldots, p_w$. The access structure Γ has a basis $\sum$ consisting of a number of 2-sets from P. The secret to be determined is an integer q in the range $2 \leq q \leq n$.

The secret information distributed to p_i is a sequence of $n(w-1)$ symbols a^i_{jk}, in the order

$$a^i_{11}, a^i_{12}, \ldots, a^i_{1n}, a^i_{21}, a^i_{22}, \ldots, a^i_{2n}, \ldots, a^i_{wn},$$

[1]This research was supported in part by the National Security Agency under Grant No. MDA904-89-H-2048 and by the Office of Research and Development Administration of Southern Illinois University under a Summer Research Grant. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon.

where k ranges from 1 to n and j ranges from 1 to w except that case $j = i$ is omitted. The $n(w-1)w$ symbols chosen for the w participants should all be different, except for the rules:

$$(1) \qquad a^i_{j1} = a^j_{i1} \text{ for all } i, j,$$

$$(2) \qquad a^i_{jq} = a^j_{iq} \text{ if } \{P_i, P_j\} \in \sum.$$

The nature of the symbols is not important - perhaps a sufficiently large set of integers, in random order, could be used.

Suppose $\{P_i, P_j\}$ is in $\sum$. When they pool their shares, they find two common elements. To determine q, they count off the sequence elements from one common element to the next, inclusive. If $\{P_i, P_j\}$ is not in $\sum$, they gain no information about q. So the system is perfect, and clearly extrinsic. We have

THEOREM: Any access structure having a basis consisting entirely of 2-sets can be realized by a perfect extrinsic secret sharing system. #

Benaloh and Leichter [1] show that there exist monotone access structures for which no ideal scheme is possible. In fact their proof involves showing that there is no ideal realization of the structure with basis

$$\{A, B\}, \qquad \{B, C\}, \qquad \{C, D\}.$$

However, we have proven that a perfect extrinsic realization does exist. So the problem of whether all monotone access structures can be realized by a perfect extrinsic scheme is still open.

Finally, we observe that our construction can be broadened to include the possibility of certain individuals who can determine the secret alone. One simply adds a new participant p_0, and adds to the set $\sum$ all the pairs $\{p_0, p_i\}$ where p_i alone can determine the secret. Finally, p_0's share is made public knowledge.

REFERENCES

1. J. Benaloh and J. Leichter, *Generalized secret sharing and monotone functions*, Advances in Cryptology (to appear).
2. E. F. Brickell, *Some ideal secret sharing schemes*, J. Combin. Math. Combin. Comput. 6 (1989), 105–113.
3. G. J. Simmons, *How to (really) share a secret*, Advances in Cryptology (to appear).
4. G. J. Simmons, *Prepositioned shared secret and/or shared control schemes*, Advances in Cryptology (to appear).