SECRET SHARING SCHEME REALIZING GENERAL ACCESS STRUCTURE

MITSURU ITO, AKIRA SAITO and TAKAO NISHIZEKI

Department of Electrical Communications, Tohoku University
Sendai, Miyagi 980, Japan

ABSTRACT

A secret sharing scheme is one of the various methods to protect a secret data d from leakage. In a scheme, a data d is broken into pieces which are shared by a set P of trustees. The family $\{P' \subset P: P'$ can reconstruct the data $d\}$ is called the access structure of the secret sharing scheme. Shamir's (k, n)-threshold scheme can realize only the access structure $\{P' \subset P: |P'| \geq k\}$. This paper provides a new methodology to design a secret sharing scheme realizing any given access structure.

Data communication systems and computer networks have been remarkably developed in recent years. Various types of data are accessed through networks. In this situation it is necessary to protect a secret data from leakage. Thus data security has become a serious issue nowadays.

A secret sharing scheme is one of strategies for data protection. It is described as follows: There are a secret data d and a set of persons $P = \{p_1, \ldots, p_n\}$. The data d is broken into n pieces $d_1, \ldots, d_n$, called *shadows*, and each d_i is distributed to p_i $(1 \leq i \leq n)$, in such a way that

(1) if $P' = \{p_{i_1}, \ldots, p_{i_l}\} \subset P$ is a qualified subset of persons, then d can be reconstructed from their shadows $\{d_{i_1}, \ldots, d_{i_l}\}$, and

(2) if $P' = \{p_{i_1}, \ldots, p_{i_l}\} \subset P$ is not a qualified subset, then d cannot be reconstructed from their shadows $\{d_{i_1}, \ldots, d_{i_l}\}$.

The family of all the qualified subsets is called the *access structure of the scheme.*

Here, we introduce set-theoretic notation for further arguments. For a set S, we denote by $|S|$ the cardinality of S and by 2^S the power set of S. Let $\mathcal{A} \subset 2^S$. The family of maximal sets in $\mathcal{A}$ is denoted by $\partial^+\mathcal{A}$:

$$\partial^+\mathcal{A} = \{A \in \mathcal{A}: A \not\subset A' \text{ for all } A' \in \mathcal{A} - \{A\}\}.$$

If P' is a qualified subset, then any subset P'' with $P' \subset P''$ must be so. Thus we have:

PROPOSITION 1. *If $\mathcal{A} \subset 2^P$ is an acccess structure of a scheme, then $\mathcal{A}$ satisfies*

(A) *$A \in \mathcal{A}$ and $A \subset A' \subset P$ imply $A' \in \mathcal{A}$.*

Shamir [3] has proposed a secret sharing scheme based on Lagrange interpolating polynomials. His scheme is called *Shamir's (k, n)-threshold scheme*, which is described as follows.

Shamir's (k,n)-Threshold Scheme

(1) Choose a prime power q such that $q > n$ and let $K = \mathrm{GF}(q)$. Also choose distinct elements $x_1, \ldots, x_n \in K - \{0\}$ randomly.

(2) Choose $a_1, \ldots, a_{k-2} \in K$ and $a_{k-1} \in K - \{0\}$ randomly, where $k \leq n$.

(3) Let $f(x) = d + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$.

(4) Let $d_i = f(x_i)$ and assign (x_i, d_i) to p_i for each i, $1 \leq i \leq n$.

In Shamir's (k, n)-threshold scheme, a set of persons $P' \subset P$ can construct the secret data d if $|P'| \geq k$. In other words, Shamir's (k, n)-threshold scheme has an access structure $\{P' \subset P: |P'| \geq k\}$. A secret sharing scheme having this access structure is generally called a *(k, n)-threshold scheme.* Realizations of a (k, n)-threshold schemes other than Shamir's have been known [1, Section 3.8]. See also [2], [4], and [5] for secret sharing schemes realizing more general access structures.

Let P be a set of persons and let $\mathcal{A} \subset 2^P$ be an arbitrary family satisfying (A) above. Our first problem is:

Problem 1. *Given $\mathcal{A}$ satisfying (A), how can one realize a scheme having an access structure $\mathcal{A}$?*

Our idea is very simple. We assign several shadows of a (k, n)-threshold scheme to each person. Formally, it is described as follows.

Multiple Assignment Scheme

(1) Choose two integers k, m and a prime power q such that $k \leq m < q$, and let $K = \mathrm{GF}(q)$.

(2) Choose $a_1, \ldots, a_{k-2} \in K$ and $a_{k-1} \in K - \{0\}$ randomly.

CH2520-5/87/0000-0099 $1.00©1987 IEEE

(3) Let $f(x) = d + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$.

(4) Choose distinct elements $x_1, \ldots, x_m \in K - \{0\}$, let $d_j = f(x_j)$ $(1 \leq j \leq m)$, and let $S = \{(x_1, d_1), \ldots, (x_m, d_m)\}$.

(5) Choose $D_i \subset S$ $(1 \leq i \leq n)$, and assign D_i to p_i for each i, $1 \leq i \leq n = |P|$.

The assignment of D_i to p_i is considered as a function $g: P \longrightarrow 2^S$ such that $g(p_i) = D_i$. Clearly the multiple assignment scheme has the following access structure $\mathcal{A}$:

$$\mathcal{A} = \left\{ Q \subset P: \left| \bigcup_{p \in Q} g(p) \right| \geq k \right\}.$$

The standard (k, n)-threshold scheme is viewed as a special case in which every $g(p)$ is a singleton set.

Our first and main theorem claims that any family $\mathcal{A} \subset 2^P$ satisfying the trivial necessary condition (A) can be realized as an access structure of a multiple assignment scheme. In general we define $\mathcal{A}(g, k)$ for finite sets P and S, a function $g: P \longrightarrow 2^S$ and a nonnegative integer k by

$$\mathcal{A}(g, k) = \left\{ Q \subset P: \left| \bigcup_{p \in Q} g(p) \right| \geq k \right\}.$$

Paticularly when S is a set of shadows of a $(k, |S|)$-threshold scheme, $\mathcal{A}(g, k)$ is exactly an access structure of the multiple assignment scheme defined by S and g.

THEOREM 1. *Let P be a set (of persons). For any $\mathcal{A} \subset 2^P$ satisfying (A), there exist a set S, a function $g: P \longrightarrow 2^S$ and a nonnegative integer k such that $\mathcal{A}(g, k) = \mathcal{A}$.*

PROOF. Let $\mathcal{B} = 2^P - \mathcal{A}$. By (A), $\mathcal{B}$ satisfies the following property:

(B) $B \in \mathcal{B}$ and $B' \subset B$ imply $B' \in \mathcal{B}$.

We now construct a set S so that each element of S corresponds one-to-one to a maximal set of $\mathcal{B}$. That is, we define

$$S = \{d_B: B \in \partial^+ \mathcal{B}\},$$

where $d_B \neq d_{B'}$ if B and $B' \in \partial^+ \mathcal{B}$ are distinct. Define $g: P \longrightarrow 2^S$ by

$$g(p) = \{d_B: B \in \partial^+ \mathcal{B},\ p \notin B\}.$$

We claim $\mathcal{A}(g, k) = \mathcal{A}$ if $k = |\partial^+ \mathcal{B}| = |S|$.

We first show $\mathcal{A} \subset \mathcal{A}(g, k)$. Assume to the contrary that there exists $Q \in \mathcal{A}$ such that $Q \notin \mathcal{A}(g, k)$. Then $\bigcup_{p \in Q} g(p) \neq S$ since $k = |S|$. Thus $d_B \in S - \bigcup_{p \in Q} g(p)$ for some $B \in \partial^+ \mathcal{B}$. Therefore for every $p \in Q$, $d_B \notin g(p)$ and so $p \in B$. Hence $Q \subset B$. By the property (b) $Q \in \mathcal{B}$. Thus $Q \in \mathcal{A} \cap \mathcal{B}$, contradicting the definition of $\mathcal{B}$.

Next, we show that $\mathcal{A}(g, k) \subset \mathcal{A}$. Assume to the contrary that there exists $Q \in \mathcal{A}(g, k)$ such that $Q \notin \mathcal{A}$. Since $Q \notin \mathcal{A}$, $Q \in \mathcal{B}$ and hence $Q \subset B$ for some $B \in \partial^+ \mathcal{B}$. By the definition of g, $d_B \notin g(p)$ for all $p \in Q$. Therefore $d_B \notin \bigcup_{p \in Q} g(p)$, and hence $Q \notin \mathcal{A}(g, k)$, a contradiction. ■

By Theorem 1, we may call a family $\mathcal{A} \subset 2^P$ an *access structure* (of some multiple assignment scheme) if $\mathcal{A}$ satisfies (A).

Next, we investigate the case in which a required access structure $\mathcal{A}$ is not fully but partially described. That is, consider the case in which $\mathcal{A}_0$ and $\mathcal{B}_0 \subset 2^P$ are given; $\mathcal{A}_0$ is a family of sets which should be contained in an access structure, while $\mathcal{B}_0$ is a family of sets which should not be contained in an access structure. Our second problem is formalized as follows.

Problem 2. *Given $\mathcal{A}_0$, $\mathcal{B}_0 \subset 2^P$, does there exist an access structure $\mathcal{A} \subset 2^P$ such that $\mathcal{A}_0 \subset \mathcal{A}$ and $\mathcal{B}_0 \subset 2^P - \mathcal{A}$?*

The next theorem presents a necessary and sufficient condition for the existence of such an access structure.

THEOREM 2. *Let $\mathcal{A}_0$, $\mathcal{B}_0 \subset 2^P$. Then there exists an access structure $\mathcal{A}$ such that $\mathcal{A}_0 \subset \mathcal{A}$ and $\mathcal{B}_0 \subset 2^P - \mathcal{A}$ if and only if*

(C) *$A \not\subset B$ for all $A \in \mathcal{A}_0$ and $B \in \mathcal{B}_0$.*

PROOF. *Necessity:* Assume that there exists an access structure $\mathcal{A}$ such that $\mathcal{A}_0 \subset \mathcal{A}$ and $\mathcal{B}_0 \bigcap \mathcal{A} = \emptyset$. Assume further that $A \subset B$ for some $A \in \mathcal{A}_0$ and $B \in \mathcal{B}_0$. Since $A \subset B$ and $A \in \mathcal{A}$, $B \in \mathcal{A}$. So $B \in \mathcal{B}_0 \bigcap \mathcal{A}$, a contradiction.

Sufficiency: Suppose that the condition (C) holds. Define $\mathcal{A}_0^-$ as

$$\mathcal{A}_0^- = \{A \subset P: A' \subset A \text{ for some } A' \in \mathcal{A}_0\}.$$

Then clearly $\mathcal{A}_0^-$ satisfies (A) and hence is an access structure. Also evidently $\mathcal{A}_0 \subset \mathcal{A}_0^-$. The only thing we have to see is $\mathcal{B}_0 \bigcap \mathcal{A}_0^- = \emptyset$. Assume $\mathcal{B}_0 \bigcap \mathcal{A}_0^- \neq \emptyset$, say $Q \in \mathcal{B}_0 \cap \mathcal{A}_0^-$. Since $Q \in \mathcal{A}_0^-$, there exists $A \in \mathcal{A}_0$ such that $A \subset Q$. However, this contradicts (C) since $Q \in \mathcal{B}_0$. ■

Given $\mathcal{A}_0$, $\mathcal{B}_0 \subset 2^P$ satisfying (C), we can realize the required access structure by first finding an access structure $\mathcal{A}_0^-$ and then realizing it by the multiple assignment scheme. However, a simpler way exists, as shown in the following theorem.

THEOREM 3. *Suppose that $\mathcal{A}_0$ and $\mathcal{B}_0 \subset 2^P$ satisfy (C). Let $S = \{d_B: B \in \partial^+ \mathcal{B}_0\}$ $(d_B \neq d_{B'}$ if $B \neq B')$,*

and let $k = |S|$. *Define* $g: P \longrightarrow 2^S$ *by*

$$g(p) = \{d_B : B \in \partial^+\mathcal{B}_0, p \notin B\}.$$

Then $\mathcal{A}_0 \subset \mathcal{A}(g,k)$ *and* $\mathcal{B}_0 \subset 2^P - \mathcal{A}(g,k)$. ■

The proof is omitted since it is similar to that of Theorem 1. Note that $\mathcal{A}_0^-$ in the proof of Theorem 2 is not always equal to $\mathcal{A}(g,k)$ in Theorem 3.

A multiple assignment scheme constructed in the proof of Theoorem 1 uses $|\partial^+\mathcal{B}|$ shadows. In some cases $|\partial^+\mathcal{B}|$ may become very large compared with $|P|$, the number of persons.

This scheme is flexible for the case in which a new member joins in P. Suppose that a multiple assignment scheme realizes an access structure $\mathcal{A}_1 \subset 2^{P_1}$ on a set of persons P_1, with an assignment function $g_1: P_1 \longrightarrow 2^{S_1}$. Suppose further that new members $p_1', \ldots, p_r'$ join in P_1, and that $\mathcal{A}_1$ is extended into a new access structure $\mathcal{A}_2$ on $P_2 = P_1 \cup \{p_1', \ldots, p_r'\}$. Our third problem is:

Problem 3. *Can a scheme realizing* $\mathcal{A}_1$ *be easily updated so that a new scheme realizes* $\mathcal{A}_2$*?*

The answer is affirmative if the new access structure $\mathcal{A}_2$ is a natural extension of $\mathcal{A}_1$, that is, $\mathcal{A}_1 \subset \mathcal{A}_2$ and $\mathcal{B}_1 \subset \mathcal{B}_2$, where $\mathcal{B}_i = 2^{P_i} - \mathcal{A}_i$ $(i = 1, 2)$. We can realize such a structure $\mathcal{A}_2$ by modifying and extending g_1 and S_1.

LEMMA 1. *Let* P_1 *and* P_2 *be sets (of persons) such that* $P_1 \subset P_2$, *let* $\mathcal{A}_i \subset 2^{P_i}$ $(i = 1, 2)$ *be an access structure, and let* $\mathcal{B}_i = 2^{P_i} - \mathcal{A}_i$ $(i = 1, 2)$. *Suppose* $\mathcal{A}_1 \subset \mathcal{A}_2$ *and* $\mathcal{B}_1 \subset \mathcal{B}_2$. *Then for every* $B_1 \in \partial^+\mathcal{B}_1$ *there exists* $B' \subset P_2 - P_1$ *such that* $B_1 \cup B' \in \partial^+\mathcal{B}_2$.

PROOF. Let $B_1 \in \partial^+\mathcal{B}_1$. Then $B_1 \in \mathcal{B}_1$. Since $\mathcal{B}_1 \subset \mathcal{B}_2$, $B_1 \in \mathcal{B}_2$. Therefore there exists $B_2 \in \partial^+\mathcal{B}_2$ such that $B_1 \subset B_2$. Now the only thing we have to see is $B' = B_2 - B_1 \subset P_2 - P_1$. Assume $B' \not\subset P_2 - P_1$. Then $B' \cap P_1 \neq \emptyset$, say $p_1 \in B' \cap P_1$. Since $p_1 \in B_2 - B_1$ and $B_1 \in \partial^+\mathcal{B}_1$, $B_1 \cup \{p_1\} \notin \mathcal{B}_1$. Since $B_1 \cup \{p_1\} \subset P_1$, $B_1 \cup \{p_1\} \in \mathcal{A}_1 \subset \mathcal{A}_2$. However, since $p_1 \in B_2$ and $B_1 \subset B_2$, $B_1 \cup \{p_1\} \subset B_2$. Since $B_2 \in \partial^+\mathcal{B}_2$, $B_1 \cup \{p_1\} \in \mathcal{B}_2$. Now we have $B_1 \cup \{p_1\} \in \mathcal{A}_2 \cap \mathcal{B}_2$, a contradiction. ■

Note that $|\partial^+\mathcal{B}_1| \leq |\partial^+\mathcal{B}_2|$ by Lemma 1.

THEOREM 4. *Let* P_i, $\mathcal{A}_i$, $\mathcal{B}_i$ $(i = 1, 2)$ *be as in Lemma 1. Let* $S_1 = \{d_B : B \in \partial^+\mathcal{B}_1\}$, *and define* $g_1: P_1 \longrightarrow 2^{S_1}$ *by* $g_1(p) = \{d_B : B \in \partial^+\mathcal{B}_1, p \notin B\}$. *(Then* $\mathcal{A}(g_1, |S_1|) = \mathcal{A}_1$ *by Theorem 1.) In this situation* $S_2 = \{d_B : B \in \partial^+\mathcal{B}_2\}$ *and* $g_2: P_2 \longrightarrow 2^{S_2}$ *can be chosen so that*

(a) $S_1 \subset S_2$,

(b) $g_1(p) \subset g_2(p)$ *for every* $p \in P_1$, *and*

(c) $\mathcal{A}(g_2, |S_2|) = \mathcal{A}_2$.

PROOF. By Lemma 1, for every $B \in \partial^+\mathcal{B}_1$, there exists $Q_B \subset P_2 - P_1$ such that $B \cup Q_B \in \partial^+\mathcal{B}_2$. We extend the set S_1 to a set S_2 by choosing $d_{B \cup Q_B} \in S_2$ so that $d_{B \cup Q_B} = d_B \in S_1$. Now we define $g_2: P_2 \longrightarrow 2^{S_2}$ as in the proof of Theorem 1:

$$g_2(p) = \{d_B : B \in \partial^+\mathcal{B}_2, p \notin B\}.$$

Clearly (a) and (c) holds, so we should show that (b) holds. Let $p \in P_1$ and $d_B \in g_1(p)$. Then $B \in \partial^+\mathcal{B}_1$ and $p \notin B$. Since $p \in P_1$, $p \notin B \cup Q_B \in \partial^+\mathcal{B}_2$. Hence $d_{B \cup Q_B} = d_B \in g_2(p)$. Thus $g_1(p) \subset g_2(p)$. ■

By Theorem 4, when a new access structure $\mathcal{A}_2$ on P_2 is a natural extension of $\mathcal{A}_1$ on P_1, the new assignment function can be obtained simply by adding several new shadows to each member of P_2. Thus one can update the scheme without ridding old members of possessed shadows.

However, we must consider one more. Theorem 4 says nothing about how to realize access structures $\mathcal{A}_1$ and $\mathcal{A}_2$ using S_1 and S_2. $\mathcal{A}_1$ is realized by using an $(|S_1|, |S_1|)$-threshold scheme, while $\mathcal{A}_2$ by an $(|S_2|, |S_2|)$-threshold scheme. So we must alter the scheme when we extend $\mathcal{A}_1$ to $\mathcal{A}_2$. This can be done as follows.

Assume that $\mathcal{A}_1$ is realized by the multiple assignment scheme with $k = m = |S_1|$. Let $k' = |S_2|$. Then $k \leq k'$ by the note after the proof of Lemma 1. Suppose that S_1 is defined by $f_1(x) = d + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$, i.e. $S_1 = \{(x_i, f_1(x_i)) : 1 \leq i \leq k\}$, where $x_1, \ldots, x_k \in K$ are distinct and $a_1, \ldots, a_{k-1} \in K$ are chosen randomly $(a_{k-1} \neq 0)$. When we extend an access structure, we first take $a_1', \ldots, a_{k'-1}' \in K$ randomly, but under the condition that $a_{k'-1}' \neq 0$ and that $f_2(x) = d + a_1' x + a_2' x^2 + \cdots + a_{k'-1}' x^{k'-1}$ satisfies $f_2(x_i) = f_1(x_i)$ $(1 \leq i \leq k)$. Next, take distinct elements $x_{k+1}, \ldots, x_{k'} \in K - \{0, x_1, \ldots, x_k\}$ and set $S_2 = \{(x_i, f_2(x_i)) : 1 \leq i \leq k'\}$. Then S_2 has the desired property. Such a alteration is possible in most cases. More formally, this alteration can be done if $k' \neq k+1$ and $k' \leq q-1$. To see this, note that the condition $f_2(x_i) = f_1(x_i)$ $(1 \leq i \leq k)$ is equivalent to

$$\begin{pmatrix} 1 & x_1 & \ldots & x_1^{k'-2} \\ 1 & x_2 & \ldots & x_2^{k'-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & \ldots & x_k^{k'-2} \end{pmatrix} \begin{pmatrix} a_1' - a_1 \\ a_2' - a_2 \\ \vdots \\ a_{k-1}' - a_{k-1} \\ a_k' \\ \vdots \\ a_{k'-1}' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

If $k' \geq k+2$, then the $k \times (k'-1)$ matrix above has rank $k < k'-1$, and hence one can select $a'_1, \ldots, a'_{k'-1}$ as desired. If $k' \leq q-1$, one can trivially select $x_{k+1}, \ldots, x_{k'}$. On the other hand, if $k' = k$, then we need not change S_1. (If $k' = k+1$, then the condition $f_1(x_i) = f_2(x_i)$ $(1 \leq i \leq k)$ forces $a'_{k'-1} = 0$, and the degree of the polymnomial $f_2(x)$ would be less than $k'-1$.)

In this paper, we have shown that the multiple assignment scheme can realize any access structure. However, the number of shadows used in the scheme might be quite large although it is bounded from above by $|\partial^+ \mathcal{B}|$ where $\mathcal{B}$ is the complement of the access structure.

References

[1] D. E. Denning, Cryptography and Data Security, Addison-Wesley, 1983.

[2] K. Koyama, *Cryptographic key sharing methods for multi-groups and security analysis*, Trans. IECE Japan, **E66, 1** (1983), 13-20.

[3] A. Shamir, *How to share a secret*, CACM **22** (1979), 612-613.

[4] T. Uehara, T. Nishizeki, E. Okamoto, and K. Nakamura, *Secret sharing systems with matroidal schemes*, Trans. IECE Japan, **J69-A, 9** (1986), 1124-1132.

[5] H. Yamamoto, *On secret sharing systems using (k, L, n) threshold scheme*, Trans. IECE Japan **J68-A, 9** (1985), 945-952.