J. Cryptology (1993) 6: 15–20

Journal of Cryptology

Multiple Assignment Scheme for Sharing Secret*

Mitsuru Ito
Mitsubishi Co., Kamimachiya 325, Kamakura-shi, Kanagawa 247, Japan

Akira Saito
Department of Mathematics, Nihon University,
Sakurajosui 3-25-40, Setagaya-ku, Tokyo 156, Japan

Takao Nishizeki
Department of Information Engineering, Faculty of Engineering,
Tohoku University, Sendai, Miyagi 980, Japan

Communicated by Ernest F. Brickell

Received 26 January 1988 and revised 12 September 1991

Abstract. In a secret sharing scheme, a datum d is broken into shadows which are shared by a set of trustees. The family $\{P' \subseteq P\colon P'$ can reconstruct $d\}$ is called the access structure of the scheme. A (k, n)-threshold scheme is a secret sharing scheme having the access structure $\{P' \subseteq P\colon |P'| \geq k\}$. In this paper, by observing a simple set-theoretic property of an access structure, we propose its mathematical definition. Then we verify the definition by proving that every family satisfying the definition is realized by assigning two more shadows of a threshold scheme to trustees.

Key words. Secret sharing, Access structure, Threshold scheme, Sperner family.

1. Introduction

A secret sharing scheme is one of various methods to protect a secret datum from leakage. It is described as follows: There are a secret datum d and a set of trustees $P = \{p_1, \ldots, p_n\}$. The datum 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 $P' = \{p_{i_1}, \ldots, p_{i_t}\} \subseteq P$ is a qualified subset of trustees, then d can be reconstructed from their shadows $\{d_{i_1}, \ldots, d_{i_t}\}$;
(2) otherwise, no information about d is obtained from their shadows.

* This work was partly supported by the Telecommunications Advancement Foundation. Also the work of the second author was partly supported by the Grant in Aid for Scientific Research of the Ministry of Education, Science and Culture of Japan under Grant Number YSE (A) 62780017.

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

A (k, n)-threshold scheme is a secret sharing scheme having the access structure $\{Q \subseteq P: |Q| \geq k\}$. Several methods to realize a (k, n)-threshold scheme have been known. See Section 3.8 of [1]. Shamir proposed a (k, n)-threshold scheme based on the Lagrange interpolation of polynomials [3]. In [3] he also noted that a hierarchical scheme may be realized by assigning two or more shadows to trustees in proportion to their importance. We call such a scheme the *multiple assignment scheme*. These previous results lead us to the following question: What family of a set can be an access structure of a secret sharing scheme?

In this paper we first propose a mathematical definition of an access structure. Then we show that any family satisfying this definition is realized by a multiple assignment scheme. For related works, we refer the reader to [2], [5], [6], and [7].

We now 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. For $\mathfrak{A} \subseteq 2^S$, the family of maximal sets in $\mathfrak{A}$ is denoted by $\partial^+\mathfrak{A}$:

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

We also define $\mathfrak{A}^-$ by

$$\mathfrak{A}^- = \{A' \in 2^S: A \subseteq A' \text{ for some } A \in \mathfrak{A}\}.$$

2. Access Structure of Multiple Assignment Scheme

In this section we first propose a formal definition of an access structure. If P' is a qualified subset of P, then any subset P'' with $P' \subseteq P'' \subseteq P$ must be so since P'' has all the information that P' has. This observation tempts us to give the following set-theoretic definition of an access structure.

Definition 1. $\mathfrak{A} \subseteq 2^P$ is said to be an access structure if $\mathfrak{A}$ satisfies

$$A \in \mathfrak{A} \quad \text{and} \quad A \subseteq A' \subseteq P \quad \text{imply} \quad A' \in \mathfrak{A}. \tag{A}$$

However, when we give the above definition, we have to prove its validity. Though it is mathematically well defined, we have to check that every family satisfying (A) can be realized by some secret sharing scheme. This is the main purpose of the paper, and we prove that it is realized by a multiple assignment scheme.

Consider a multiple assignment scheme based on a (k, m)-threshold scheme for some k and m with $k \leq m$. Let S be the set of shadows of the (k, m)-threshold scheme, where $|S| = m$. A multiple assignment scheme assigns a set $S_i \subseteq S$ of shadows to a trustee $p_i \in P$. The assignment can be viewed as a function $g: P \to 2^S$ such that $g(p_i) = S_i$. (Hence the shadow of p_i is $g(p_i)$ here.) This function is called an *assignment function*. If $Q \subseteq P$ satisfies $|\bigcup_{p \in Q} g(p)| \geq k$, then Q has k or more shadows of S which has the structure of the (k, m)-threshold scheme. Hence Q can reconstruct the secret. On the other hand, if Q satisfies $|\bigcup_{p \in Q} g(p)| < k$, then Q has less than k shadows of S. Again since S has the structure of the (k, m)-threshold scheme, Q gets no information about the secret. Therefore, the access structure is $\{Q \subseteq P: |\bigcup_{p \in Q} g(p)| \geq k\}$. This access structure is determined by S, g, and k, and is denoted by $\mathfrak{A}(S, g, k)$. If the image $g(p_i)$ of each p_i is a singleton set and $g(p_i) \neq g(p_j)$ for $i \neq j$ holds, then the scheme is exactly a $(k, |P|)$-threshold scheme. Hence a multiple assignment scheme is a generalization of a threshold scheme.

Our main theorem claims that any family $\mathfrak{A} \subseteq 2^P$ satisfying (A) can be realized by a multiple assignment scheme.

Theorem 1. *Let P be a set (of trustees). For any $\mathfrak{A} \subseteq 2^P$ satisfying* (A), *there exists a multiple assignment scheme of an access structure $\mathfrak{A}$.*

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

$$B \in \mathfrak{B} \quad \text{and} \quad B' \subseteq B \quad \text{imply} \quad B' \in \mathfrak{B}. \tag{B}$$

We give a realization of $\mathfrak{A}$, using a (k, m)-threshold scheme with $k = m = |\partial^+\mathfrak{B}|$. Let S be a set of shadows of an (m, m)-threshold scheme, where $m = |\partial^+\mathfrak{B}|$. Let $S = \{s_1, \ldots, s_m\}$ and $\partial^+\mathfrak{B} = \{B_1, \ldots, B_m\}$. Since $|S| = |\partial^+\mathfrak{B}|$, we can establish a one-to-one correspondence between S and $\partial^+\mathfrak{B}$ by assigning $s_i \in S$ to each $B_i \in \partial^+\mathfrak{B}$. Define $g\colon P \to 2^S$ by

$$g(p) = \{s_i\colon p \notin B_i\}.$$

We claim $\mathfrak{A}(S, g, k) = \mathfrak{A}$.

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

Next, we show that $\mathfrak{A}(S, g, k) \subseteq \mathfrak{A}$. Assume to the contrary that there exists $Q \in \mathfrak{A}(S, g, k)$ such that $Q \notin \mathfrak{A}$. Since $Q \notin \mathfrak{A}$, $Q \in \mathfrak{B}$ and hence $Q \subseteq B_i$ for some $B_i \in \partial^+\mathfrak{B}$. By the definition of g, $s_i \notin g(p)$ for all $p \in Q$. Therefore, $s_i \notin \bigcup_{p \in Q} g(p)$, and hence $Q \notin \mathfrak{A}(S, g, k)$, a contradiction. Thus, the claim is proved.

By the equation $\mathfrak{A}(S, g, k) = \mathfrak{A}$ and the fact that $m - 1$ or fewer elements of S give no information about the secret, this multiple assignment scheme precisely realizes $\mathfrak{A}$. □

Next, we consider the case in which a required access structure $\mathfrak{A}$ is not completely but partially described. Thus let $\mathfrak{A}_0$ and $\mathfrak{B}_0$ be given: $\mathfrak{A}_0$ is a family of sets which should be contained in an access structure $\mathfrak{A}$, while $\mathfrak{B}_0$ is a family of sets which should not be contained in $\mathfrak{A}$. The next theorem presents a necessary and sufficient condition for the existence of an access structure $\mathfrak{A}$ such that $\mathfrak{A}_0 \subseteq \mathfrak{A}$ and $\mathfrak{B}_0 \subseteq 2^P - \mathfrak{A}$.

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

$$A \nsubseteq B \qquad \textit{for all} \quad A \in \mathfrak{A}_0 \quad \textit{and} \quad B \in \mathfrak{B}_0. \tag{C}$$

Proof. (*Necessity*) Assume that there exists an access structure $\mathfrak{A}$ such that $\mathfrak{A}_0 \subseteq \mathfrak{A}$ and $\mathfrak{B}_0 \cap \mathfrak{A} = \varnothing$. Assume further that $A \subseteq B$ for some $A \in \mathfrak{A}_0$ and $B \in \mathfrak{B}_0$. Since $A \subseteq B$ and $A \in \mathfrak{A}$, $B \in \mathfrak{A}$. So $B \in \mathfrak{B}_0 \cap \mathfrak{A}$, a contradiction.

(*Sufficiency*) Suppose that condition (C) holds. Clearly, $\mathfrak{A}_0^-$ satisfies condition (A) and hence is an access structure. Also evidently $\mathfrak{A}_0 \subseteq \mathfrak{A}_0^-$. The only thing we have to prove is $\mathfrak{B}_0 \cap \mathfrak{A}_0^- = \emptyset$. Assume $\mathfrak{B}_0 \cap \mathfrak{A}_0^- \neq \emptyset$, and let $Q \in \mathfrak{B}_0 \cap \mathfrak{A}_0^-$. Since $Q \in \mathfrak{A}_0^-$, there exists $A \in \mathfrak{A}_0$ such that $A \subseteq Q$. However, this contradicts (C) since $Q \in \mathfrak{B}_0$. □

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

Theorem 3. *Suppose that $\mathfrak{A}_0$ and $\mathfrak{B}_0 \subseteq 2^P$ satisfy* (C). *Let $\partial^+\mathfrak{B}_0 = \{B_1, \ldots, B_m\}$, $S = \{s_1, \ldots, s_m\}$, and $k = |S|$. Define g: $p \rightarrow 2^P$ by*

$$g(p) = \{s_i : p \notin B_i\}.$$

Then $\mathfrak{A}_0 \subseteq \mathfrak{A}(S, g, k)$ and $\mathfrak{B}_0 \subseteq 2^P - \mathfrak{A}(S, g, k)$.

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

We do not claim that the method shown in the proof of Theorem 1 is the only one to realize a given access structure by a multiple assignment scheme, nor do we claim that it is the best one. For some access structure $\mathfrak{A}$, there exist two or more different realizations of $\mathfrak{A}$. For example, if we realize the access structure of a (k, n)-threshold scheme by the method in the proof of Theorem 1, we need $\binom{n}{k}$ shadows. Of course, we can realize this access structure by using n shadows of an ordinary (k, n)-threshold scheme, which is a special case of a multiple assignment scheme.

The multiple assignment scheme constructed in the proof of Theorem 1 uses $|\partial^+\mathfrak{B}|$ shadows. In some cases $|\partial^+\mathscr{B}|$ may become very large compared with $|P|$, the number of trustees. Here we give an upper bound of $|\partial^+\mathfrak{B}|$. Before presenting the bound, we introduce the notion of a Sperner family and present a classical result on the set theory. A family $\mathfrak{A} \subseteq 2^P$ is said to be a *Sperner family* if every two distinct sets in $\mathfrak{A}$ are incomparable:

$$A \not\subset A' \qquad \text{for any} \quad A, A' \in \mathfrak{A}.$$

Sperner [4] showed the following result.

Theorem 4 [4]. *If $\mathfrak{A} \subseteq 2^P$ is a Sperner family, then*

$$|\mathfrak{A}| \leq \binom{|P|}{\lfloor |P|/2 \rfloor}.$$

Furthermore, this upper bound is sharp.

If $\mathfrak{A}$ is an access structure and $\mathfrak{B} = 2^P - \mathfrak{A}$, then $\partial^+\mathfrak{B}$ is a Sperner family. By Theorem 4, the number of shadows used in the multiple assignment scheme is bounded from above by $\binom{n}{\lfloor n/2 \rfloor}$, where n is the number of trustees. Note that, though the above bound is sharp for Sperner families, it is not a tight upper bound of the number of used shadows in the multiple assignment scheme. There may be realizations of a give access structure other than the one described in the proof of Theorem 1, as noted after Theorem 3.

3. Conclusion

In this paper we have proposed a mathematical definition of an access structure, and we have verified the definition by proving that every family satisfying the definition can be realized by a multiple assignment scheme. We have also given an upper bound on the number of shadows used by the realization. In the paper we have only made use of a (k, m)-threshold scheme with $k = m$. As one of the referees points out, such a special threshold scheme is easily constructed without using a general (k, n)-threshold scheme. This is true. We do not propose to use a (k, k)-threshold scheme to realize a given access structure. We have only proved the validity of Definition 1 as a formal definition of an access structure. We have only used a (k, k)-threshold scheme simply because we do not know the way to use a general threshold scheme to realize a given access structure. Thus the next step may be to find an efficient method to realize a given access structure which uses a smaller number of shadows. In particular, if we allow a general (k, m)-threshold scheme, removing the restriction $k = m$, then the number of shadows used may be considerably reduced. Therefore, we leave the following open problem.

Problem 1. Is it possible to lower the bound $\binom{|P|}{\lfloor |P|/2 \rfloor}$ on the number of shadows used by multiple assignment shadows if we use a (k, m)-threshold scheme, where k is not necessarily equal to m?

Problem 2. Characterize the access structures which can be realized by a multiple assignment scheme in which the number of shadows used is linear to that of the trustees.

Acknowledgments

We wish to thank Professor Nobuki Saito for stimulating discussions and encouragement. We are also grateful to one of the referees for his careful reading of the paper and valuable comments, which have led us tqward the improvement of the paper.

References

[1] D. E. Denning, *Cryptography and Data Security*, Addison-Wesley, Reading, MA, 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, *Comm. ACM* **22** (1979), 612–613.

[4] E. Sperner, Ein Sats über Untermengen einer endlichen Menge, *Math. Z.* **27** (1928), 544–548.

[5] D. R. Stinton and S. A. Vanstone, A combinatorial approach to threshold scheme, *Advances in Cryptology—Proceedings Crypto* '87 (C. Pomerrance, ed.), Lecture Notes in Computer Science, Vol. 293, Springer-Verlag, Berlin, 1988, pp. 330–339.

[6] T. Uehara, T. Nishizeki, E. Okamoto, and K. Nakamura, Secret sharing systems with matroidal schemes, *Trans. IECE Japan* **J68-A,9** (1986), 1124–1132.

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