JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 17, 959-965 (2001)

Short Paper

A New Method for Constructing Multiple Assignment Schemes for Generalized Secret Sharing

GWOBOA HORNG
Institute of Computer Science
National Chung-Hsing University
Taichung, 402 Taiwan
E-mail: gbhorng@cs.nchu.edu.tw

A secret sharing scheme is a way of protecting a secret by distributing partial information to a set of participants P in such a way that only authorized subsets of P can recover the secret. The family of authorized subsets is called the access structure of the scheme. In 1979, threshold schemes were proposed to realize threshold access structures, and in 1987, multiple assignment schemes were proposed to realize monotone access structures. In this paper, we propose a new method for constructing multiple assignment schemes. Basically, our construction method is a combination of the threshold scheme and the cumulative scheme. We also show that the new method yields better results for some special access structures.

Keywords: cryptography, secret sharing, access structure, threshold scheme, multiple assignment scheme

1. INTRODUCTION

A secret sharing scheme is a way of protecting a secret, K, by distributing partial information to a set of participants, $P = \{P_1, P_2, \ldots, P_n\}$, such that only authorized subsets of P can recover K, but any unauthorized subset can not recover K. Such schemes are useful for protecting important secret data, such as cryptographic keys, from being lost or destroyed. They are also useful for constructing shared control schemes and fault tolerance schemes. Secret sharing schemes have been extensively investigated since their invention in 1979. A detailed bibliography can be found at Stinson's homepage [1].

The secret K is known to a special person called the *dealer*. The dealer breaks K into pieces, called *shares*, and distributes a subset of the shares, called *shadows*, to each participant in such a way that

1. if $P' \subseteq P$ is an authorized subset of participants, then the participants in P' can reconstruct K from their shadows;

Received January 16, 2001; accepted July 10, 2001.
Communicated by Chi Sung Laih.

2. otherwise, they cannot reconstruct K from their shadows.

Let $\mathcal{K}$ be the set of all possible secrets. Let S be the set of shares, and let $S_i \subset S$ be the shadow distributed to participant P_i. Then the distribution of shadows to participants can be viewed as a function $G : P \rightarrow 2^S$ such that $G(P_i) = S_i$. This function is called an *assignment function* [2]. We shall assume throughout this paper that P, $\mathcal{K}$, and S are all finite sets. A secret sharing scheme is *perfect* if any unauthorized subset of participants can determine nothing about the value of K other than $K \in \mathcal{K}$. The family of authorized subsets is called the *access structure*, $\mathcal{A}$, of the scheme. That is, $\mathcal{A} = \{Q : Q \subseteq P$ and the participants in Q can recover the secret K from their shadows$\}$. An access structure $\mathcal{A}$ is said to be *monotone* if $A \in \mathcal{A}$ then $\forall B$ such that $A \subseteq B \subseteq P$, $B \in \mathcal{A}$. An authorized subset A is *minimal* if $\forall B \subset A$, $B \notin \mathcal{A}$. The set of all minimal authorized subsets of access structure $\mathcal{A}$ is denoted by $\mathcal{A}_0$. An unauthorized subset B is *maximal* if $\forall A \supset B$, $A \in \mathcal{A}$. The set of all maximal unauthorized subsets of access structure $\mathcal{A}$ is denoted by $\mathcal{B}_0$. We assume that $\forall P_i \in P, \exists Q \in \mathcal{A}$ such that $P_i \in Q$. That is, $P = \cup_{Q \in \mathcal{A}} Q$. A formal definition of secret sharing schemes can be found in [3]. Secret sharing schemes can be constructed from a variety of mathematical structures and properties, such as polynomials [4], finite geometries [5], and combinatorial designs [6].

2. THRESHOLD SCHEMES AND MULTIPLE ASSIGNMENT SCHEMES

Shamir [4] and Blakley [5] proposed methods to construct perfect secret sharing schemes such that $|S| = |P|$ and $|S_i| = 1$ for $i = 1, 2, ..., n$. Such schemes are also called (t, n)-*threshold schemes* for some threshold value t such that $1 < t \leq n$, where $n = |P|$. They can be used to realize the threshold access structures $\mathcal{A} = \{Q : Q \subseteq P$ and $|Q| \geq t\}$.

Secret sharing for general access structures was studied by Ito *et al.* [7]. Let $\mathcal{A}$ be a monotone access structure, and let m be the number of maximal unauthorized subsets, that is, $m = |\mathcal{B}_0|$. Ito, Saito, and Nishizeki proposed a realization of $\mathcal{A}$, called a *multiple assignment scheme*, using an (m, m)-threshold scheme [2]. Their construction establishes a one-to-one correspondence between the set of all shares $S = \{u_1, u_2, \ldots, u_m\}$ and the set of all maximal unauthorized subsets $\mathcal{B}_0 = \{B_1, B_2, \ldots, B_m\}$ by associating u_i with B_i. Then participant P_i is given a subset $S_i \subseteq S$ such that $S_i = \{u_j : P_i \notin B_j, 1 \leq j \leq m\}$. That is, $G(P_i) = S_i$, where $S_i = \{u_j : P_i \notin B_j, 1 \leq j \leq m\}$. In [2], the authors show that $\forall A \in \mathcal{A}, \cup_{Pi \in A} S_i = S$ and $\forall B \notin \mathcal{A}$, $\exists s \in S$ such that $s \notin \cup_{Pi \in B} S_i$. A multiple assignment scheme is also called a cumulative scheme in [8-11]. The construction scheme is illustrated by the following example:

Example 1. Let $P = \{P_1, P_2, \ldots, P_7\}$. The access structure $\mathcal{A}$ consists of all the subsets with 3 or more participants except the following three subsets $\{P_4, P_5, P_7\}$, $\{P_4, P_6, P_7\}$, and $\{P_5, P_6, P_7\}$. Then it is easy to see that $|\mathcal{B}_0| = 18$ and we can construct a multiple assignment scheme which is basically a (18, 18)-threshold scheme. ❑

Benaloh and Leichter [12] also presented an elegant construction based on a monotone circuit for any monotone access structure. Their basic approach is to build a monotone circuit from the access structure and then assign a value to every wire in the

circuit such that the output wire of the circuit is the secret K. Then each participant is given the shares corresponding to the values of the wires connecting to him. When an authorized subset A wants to reconstruct the secret, the participants in A need to know the circuit, that is, the access structure, used by the dealer to assign shares, and need to know which shares correspond to which wires of the circuit.

An advantage of multiple assignment schemes over monotone circuit constructions is that the access structure is not required during secret reconstruction by an authorized subset. However, the threshold value may be very large even for a very simple access structure. For example, we need $C(n, t - 1) = n!/((t - 1)!(n - t + 1)!)$ shares to realize a threshold access structure with threshold value t based on multiple assignment construction since the number of maximal unauthorized subsets is $C(n, t - 1)$. In fact, two open problems were proposed in [2]:

1. Is it possible to reduce the number of shares used in constructing a multiple assignment scheme if we use a (k, m) threshold scheme, where k is not necessarily equal to m?
2. Is it possible to characterize the access structures which can be realized by a multiple assignment scheme in which the number of shares used is linear to that of the participants?

In the following sections, we will give partial answers to these questions.

3. NEW CONSTRUCTION

Let $n > 1$ and $P = \{P_1, P_2, \ldots, P_n\}$ be the set of all participants. Let $\mathcal{A} \subseteq 2^P$ be a monotone access structure, let $\mathcal{A}_0$ be the set of all minimal authorized subsets, and let $\mathcal{B}_0$ be the set of all maximal unauthorized subsets. Let $t = \min_{A \in \mathcal{A}_0} \{|A|\}$, $\mathcal{A}_t = \{A : A \in \mathcal{A}_0$ and $|A| > t\}$, and let $\mathcal{B}_t = \{B : B \in \mathcal{B}_0, |B| \geq t$, and $\nexists\, A \in \mathcal{A}_0$ such that $B \subset A\}$.

Let $\mathcal{A}_t = \{A_1, A_2, \ldots, A_a\}$, and let $\mathcal{B}_t = \{B_1, B_2, \ldots, B_b\}$. Let $\alpha_i = |A_i| - t$, for all $1 \leq i \leq a$, and let $\beta_j = |B_j| - t + 1$, for all $1 \leq j \leq b$. Then it is easy to see that $\alpha_i \geq 1$ and $\beta_j \geq 1$ for all $1 \leq i \leq a$ and $1 \leq j \leq b$ since $|A_i| > t$ and $|B_j| \geq t$ by definition.

Let $m = n + \alpha + \beta$, and let $k = t + \alpha + \beta$ where $\alpha = \sum_{i=1}^{a} \alpha_i$ and $\beta = \sum_{j=1}^{b} \beta_j$. In the following, we will show how to construct a multiple assignment scheme realizing $\mathcal{A}$ based on a (k, m)-threshold scheme. Let S be the set of shares, and let $|S| = m$. S is partitioned into three subsets U, V, and W such that $U = \{u_1, u_2, \ldots, u_n\}$; $V = \bigcup_{j=1}^{b} V_j$, where $|V_j| = \beta_j$ and $V_j \cap V_k = \emptyset$ for $j \neq k$, $1 \leq j, k \leq b$; and $W = \bigcup_{i=1}^{a} W_i$, where $|W_i| = \alpha_i$ and $W_i \cap W_k = \emptyset$ for $i \neq k$, $1 \leq i, k \leq a$.

Define a function $F : 2^P \rightarrow 2^S$ such that

$$F(C) = \begin{cases} \{u_i\} & \text{if } C = \{P_i\} \text{ for } 1 \leq i \leq n \\ V_j & \text{if } C = B_j \text{ for } 1 \leq j \leq b \\ W_k & \text{if } C = A_k \text{ for } 1 \leq k \leq a \\ \emptyset & \text{otherwise.} \end{cases}$$

The share assignment function $G : P \rightarrow 2^S$ is defined as follows:

$G(P_i) = F(\{P_i\} \cup (\cup_{P_i \notin B_j} F(B_j)) \cup (\cup_{P_i \notin A_j} F(A_j))$.

In the following, we will show that the multiple assignment scheme based on this share assignment function realizes the given access structure $\mathcal{A}$ and is basically a (k, m)-threshold scheme.

For $C \subseteq P$, let $T_C = \cup_{P_i \in C} G(P_i)$.

Lemma 1. For all $A \in \mathcal{A}_0$, $|T_A| = t + \alpha + \beta$.

***Proof*:** Since $A \in \mathcal{A}_0$, we have $|A| \geq t$. If $|A| = t$; then $\forall A_i \in \mathcal{A}_t$, $B_j \in \mathcal{B}_t$, $A \not\subseteq A_i$ and $A \not\subseteq B_j$. Hence, there exist participants P_c and P_d in A such that $P_c \notin A_i$ and $P_d \notin B_j$. Therefore, $W_i \subseteq G(P_c)$ and $V_j \subseteq G(P_d)$. That is, $W_i \subseteq T_A$ and $V_j \subseteq T_A$ for all $1 \leq i \leq a$ and $1 \leq j \leq b$. Furthermore, $|T_A \cap U| = |A| = t$. Therefore, $|T_A| = t + \alpha + \beta$.

If $|A| > t$, then $A \in \mathcal{A}_t$. Therefore, $A = A_l$ for some $1 \leq l \leq$ a. Hence, $\forall A_i \in \mathcal{A}_t$, $B_j \in \mathcal{B}_t$ such that $i \neq l$, and we have $A \not\subseteq A_i$ and $A \not\subseteq B_j$. Hence, there exist participants P_c and P_d in A such that $P_c \notin A_i$ and $P_d \notin B_j$. Therefore, $W_i \subseteq G(P_c)$ and $V_j \subseteq G(P_d)$. That is, $W_i \subseteq T_A$ and $V_j \subseteq T_A$ for all $1 \leq i \leq a$, $i \neq$ l, and $1 \leq j \leq b$. Furthermore, $|T_A \cap \mathrm{U}| = |A_l|$. Therefore, $|T_A| = |A_l| + \alpha - \alpha_l + \beta = |A_l| + \alpha - (|A_l| - t) + \beta = t + \alpha + \beta$.❑

Lemma 2. For all $B \in \mathcal{B}_0$, $|T_B| < t + \alpha + \beta$.

Proof: If $|B| < t$, then $|T_B \cap U| = |B| < t$. Hence, $|T_B| < t + \alpha + \beta$.

If $|B| \geq t$, and $B \notin \mathcal{B}_t$ then $B \subset A_l$ for some $1 \leq l \leq a$. Therefore, $|T_B| \leq |B| + \beta + (\alpha - \alpha_l) \leq t + \alpha + \beta - 1$ since $W_l \not\subseteq T_B$ and $|W_l| = \alpha_l - 1$.

If $|B| \geq t$ and $\mathrm{B} \in \mathcal{B}_t$, then $\mathrm{B} = B_l$ for some $1 \leq l \leq b$. Therefore, $|T_B| \leq |B| + (\beta - \beta_l) + \alpha = t + \alpha + \beta - 1$ since $T_B \cap V_l = \emptyset$ and $\beta_l = |B| - t + 1$. ❑

Based on Lemma 1 and Lemma 2, we have the following theorem.

Theorem 1. The multiple assignment scheme based on the share assignment function G is a (k, m)-threshold scheme realizing the given monotone access structure $\mathcal{A}$.

Proof: If $A \in \mathcal{A}$, then there exists an $A' \in \mathcal{A}_0$ such that $A' \in A$. Therefore, by Lemma 1, $|T_A| \leq |T_{A'}| = k$, and the participants in A can recover the secret from their shadows.

If $A \notin \mathcal{A}$, then there exists an $B \in \mathcal{B}_0$ such that $A \subseteq B$. Therefore, by Lemma 2, $|T_A| \leq |T_B| < k$, and the participants in B can not recover the secret from their shadows. ❑

Example 2. In this example, we will illustrate use of this new construction scheme by returning to the access structure of Example 1. Based on $\mathcal{A}_0$ and $\mathcal{B}_0$, we have $t = 3$, $\mathcal{A}_t = \emptyset$, and $\mathcal{B}_t = \{\{P_4, P_5, P_7\}, \{P_4, P_6, P_7\}, \{P_5, P_6, P_7\}\}$. Following the above notation, we can construct a multiple assignment scheme realizing the given $\mathcal{A}$ as follows. Let $U = \{u_1, u_2, \ldots, u_7\}$ and $V = \{v_1, v_2, v_3\}$. Based on the construction, we have $G(P_i) = \{u_i, v_1, v_2, v_3\}$ for $i = 1$, 2 or 3, $G(P_4) = \{u_4, v_3\}$, $G(P_5) = \{u_5, v_2\}$, $G(P_6) = \{u_6, v_1\}$, and $G(P_7) = \{u_7\}$. It is easy to verify that the participants of an authorized subset together hold at

least 6 shares. For example, participants P_2, P_4, and P_6 hold six shares together, namely, u_2, u_4, u_6, v_1, v_2, and v_3. However, the participants of an unauthorized subset together hold at most 5 shares. For example, the participants in the unauthorized subset $\{P_5, P_6, P_7\}$ hold only five different shares, namely u_5, u_6, u_7, v_1, v_2. Therefore, the access structure can be realized by means of a multiple assignment scheme which is basically a (6, 10)-threshold scheme. ❑

Example 3. Let us consider a different access structure by modifying $\mathcal{A}$ slightly. Assume that the new access structure $\mathcal{A}'$ consists of all the subsets with 3 or more participants except for the following four subsets: $\{P_4, P_5, P_6\}$, $\{P_4, P_5, P_7\}$, $\{P_4, P_6, P_7\}$, and $\{P_5, P_6, P_7\}$. Then $t = 3$, $\mathcal{A}'_t = \{P_4, P_5, P_6, P_7\}$, and $\mathcal{B}'_t = \emptyset$. Therefore, we have the following share assignment function: $G(P_i) = \{u_i, w_1\}$ for $i = 1, 2, 3$, and $G(P_j) = \{u_j\}$, for $j = 4, 5, 6, 7$. The constructed multiple assignment scheme is basically a (4, 8)-threshold scheme. Note that this access structure will be realized by a (19, 19)-threshold scheme based on the construction of Ito *et al*. ❑

4. DISCUSSION

Basically, our construction approach is a combination of the threshold scheme and the cumulative scheme. The total number of different shares held by the participants of an authorized subset must consist of all the β shares in the set V together with at least $\alpha + t$ out of the $\alpha + n$ shares in the sets W and U. The threshold access structure is a special case of the general access structure with $\alpha = \beta = 0$. Based on our construction, the multiple assignment scheme realizing the threshold access structure is exactly the same as the threshold scheme.

In [13], Sun and Shieh proposed a construction for perfect secret sharing schemes with improved lower bounds on the information rate for uniform, generalized access structures of constant rank. An access structure is *uniform* if every minimal qualified subset has the same cardinality, and if the *rank* of an access structure is the maximum cardinality of a minimal qualified subset.

The examples gives in the previous section show that our new construction improves the total number of shares for realizing the given access structures. In general, if a given access structure is close to the one which a threshold scheme realizes, then our new scheme tends to use a much smaller number of shares than the original multiple assignment construction [2]. In the following, we will show that our scheme yields better multiple assignment schemes for cases where $\alpha = 0$ and β is small.

Let $\mathcal{A}$ be a uniform monotone access structure such that $\mathcal{A}_0$ consists of subsets of exactly t participants, and such that the set of all maximal unauthorized subsets $\mathcal{B}_0$ of $\mathcal{A}$ can be partitioned into two subsets V_1 and V_2, where $V_1 = \{v \in V : |v| = t\}$ and $V_2 = \{v \in V : |v| = t - 1\}$. Note that $|V_1| = \beta$. Based on the construction described in the previous section, there is a $(t + \beta, n + \beta)$-threshold scheme realizing the access structure $\mathcal{A}$.

When β is small, our construction will yield a scheme with a smaller threshold value than that of the multiple assignment scheme proposed by Ito *et al.* [2]. For example, if $\beta = 1$ then $|V_1| = 1$ and $|V_2| = \binom{n}{t-1} - t$. Therefore, the threshold value of the scheme

proposed by Ito *et al.* is $1 + \binom{n}{t-1} - t$, whereas, the threshold value of our scheme is only $t+1$.

We can derive the largest value of β such that our construction will always yield a scheme with a smaller threshold value. Let $b = |V|$. Among the $\binom{n}{t-1}$ subsets of P with cardinality $t - 1$, there are at most $\beta\binom{t}{t-1} = \beta t$ subsets that are not maximal unauthorized subsets. Hence,

$$|V_2| \geq \binom{n}{t-1} - \beta t.$$

Therefore,

$$b = |V_1| + |V_2| \geq \beta + \binom{n}{t-1} - \beta t.$$

Based on the construction proposed by Ito *et al.*, the threshold value is b. Our construction will have a smaller threshold value if $t + \beta < b$. That is,

$$t + \beta + \leq \beta + \binom{n}{t-1} - \beta t.$$

Therefore, when

$$\beta < \frac{1}{t}\binom{n}{t-1} - 1,$$

our construction will yield a scheme with a smaller threshold value than will the original multiple assignment scheme.

5. CONCLUSIONS

In this paper, we have proposed a new method for constructing a multiple assignment scheme for any monotone access structure. Basically, our method is a combination of the threshold scheme and the original multiple assignment scheme proposed in [2]. We have also shown that our method yields better results than the original multiple assignment construction for some special access structures.

REFERENCES

1. http://www.cacr.math.uwaterloo.ca/~dstinson.
2. M. Ito, A. Saito, and T. Nishizeki, "Multiple assignment scheme for sharing secret," *Journal of Cryptology*, Vol. 6, No. 1, 1993, pp. 15-20.
3. D. Stinson, *Cryptography: Theory and Practice*, CRC Press, Inc. 1995, pp. 327-360.
4. A. Shamir, "How to share a secret," *Communications of ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
5. G. Blakey, "Safeguarding cryptographic keys," in *Proceedings of American Federation of Information Processing Societies 1979 National Conference*, Vol. 48, 1979, pp. 313-317.

6. P. J. Schellenberg and D. R. Stinson, "Threshold schemes from combinatorial designs," *Journal of Combinatorial Mathematics and Combinatorial Computing*, Vol. 5, No. 4, 1989, pp. 143-160.
7. M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," in *Proceedings of IEEE Globecom* '87, 1987, pp. 99-102.
8. C. Charnes and J. Pieprzyk, "Cumulative arrays and generalized Shamir secret sharing schemes," in *Proceeding of Australian Computer Science Communications* '17, 1994, pp. 519-528.
9. H. Ghodosi, J. Pieprzyk, R. Safavi-Naini, and H. Wang, "On construction of cumulative secret sharing schemes," in *Proceedings of ACISP* '98 (*Australian Conference on Information Security and Privacy*), Lecture Notes in Computer Science, Vol. 1438 Springer-Verlag, Berlin, 1998, pp. 379-390.
10. W. Jackson and K. Martin, "Cumulative arrays and geometric secret sharing schemes," in *Proceedings of Advances in Cryptology AUSCRYPT* '92, Lecture Notes in Computer Science, Vol. 718, Springer, Berlin, 1993, pp. 48-55.
11. G. Simmons, W. Jackson, and K. Martin, "The geometry of shared secret schemes," *Bulletin of the Institute of Combinatorics and its Applications* (*ICA*), Vol. 1, 1991, pp. 71-88.
12. J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Proceedings of Cryptology CRYPT* '88, Lecture Notes in Computer Science, Vol. 403, Springer-Verlag, Berlin, 1990, pp. 27-35.
13. H. Sun and S. Shieh, "Constructing perfect secret sharing schemes for general and uniform access structures," *Journal of Information Science and Engineering*, Vol. 15 No. 5, 1999, pp. 679-689.

Gwoboa Horng (洪國寶) received the B.S. degree in Electrical Engineering from National Taiwan University in 1981 and the M.S. and Ph.D. degrees from the University of Southern California in 1987 and 1992 respectively, all in Computer Science. Since 1992, he has been on the faculty of the Institute of Computer Science at National Chung-Hsing University, Taichung, Taiwan, R.O.C. His current research interests include artificial intelligence, cryptography and information security.