

On Constructing Secret Sharing Schemes

Shiuh-Pyng Shieh and Hung-Min Sun

Department of Computer Science and Information Engineering
National Chiao Tung University
Hsinchu, Taiwan 30050

Abstract

A secret sharing scheme is a method which allows a secret to be shared among a finite set of participants in such a way that only qualified subsets of participants can recover it. A secret sharing scheme is called perfect if unqualified subsets of participants obtain no information about the secret. In this paper, we propose an efficient construction of perfect secret sharing schemes for the access structures consisting of the closure of a graph where a vertex denotes a participant and an edge denotes a minimal qualified pairs of participants. The information rate of our scheme is at least $1/(2|P|)$, where P denotes the set of the participants, which is better than $O(1/|P|^2)$ of existing schemes used for graph-based access structures. We also present an application of our scheme to the reduction of storage and computation loads on the key distribution server in a secure network.

1 Introduction

The concept of an (m, n) threshold scheme is to decompose a master key, top secret, into n shares in such a way that the master key cannot be reclaimed unless m shares are collected [1, 2]. In 1979, Shamir [3] described a general method of secret sharing called *secret sharing scheme* (SSS) which allows a secret to be shared among a finite set of participants in such a way that only qualified subsets of participants can recover the secret [3]. Let K be the master key space, S be the share space, $|K|$ be the size of the master key space, and $|S|$ be the size of the share space used in a secret sharing scheme. The information rate for the secret sharing scheme is defined to be $\log_2|K|/\log_2|S|$. We generalize this definition to be $\log_2|K|/\max\{\log_2|S_i|\}$, where S_i is the space of shares

owned by participant i . A *construction* for a secret sharing scheme is some concrete realization of the scheme. It is clear that the threshold scheme is a special case of secret sharing schemes. A secret sharing scheme is called *perfect* if unqualified subsets of participants obtain no information regarding the secret [4,5,6]. Given any monotone access structure (i.e., any subset which contains a qualified subset of participants is also qualified), Ito *et al.* showed that there exists a perfect secret sharing scheme to realize the access structure [3]. Benaloh and Leichter proposed a different algorithm to realize secret sharing schemes for any given monotone access structure [7]. In both constructions, the information rate exponentially decreases as a function of $|P|$, where P denotes the set of the participants.

There are several performance and efficiency measures proposed for construction of secret sharing schemes [8, 9]. Their goal was to maximize the information rate of a secret sharing scheme. Brickell and Stinson studied perfect secret sharing schemes for the access structures consisting of the closure of a graph where a vertex denotes a participant and an edge denotes a minimal qualified pair of participants [8]. They proved that, for any graph G with n vertices having maximum degree d , there exists a perfect secret sharing scheme realizing G in which the information rate is at least $2/(d+3)$. In the worst case when $d = n-1$, the information rate is $2/(n+2)$. Their construction is not feasible because it need maintain a large access check matrix with at least $|K| \cdot d$ rows. In this paper, we will propose an efficient construction of perfect secret sharing schemes for the access structure based on a graph. The information rate of our scheme is at least $1/(2|P|)$, where P is the set of the participants, which is better than existing schemes' $O(1/|P|^2)$ used for graph-based access structures [7,10].

In section 2, we propose a construction of perfect secret sharing schemes for graph-based access structures. In section 3, we extend the construction to cope with some

*This research was supported by National Science Council of Republic of China under grant No. NSC-82-0408-E-009-290.

special graph-based access structures. In section 4 and 5, we discuss the application of our construction, and conclude the paper, respectively.

2 Construction of perfect SSS for graph-based access structures

It is difficult to efficiently construct a secret sharing scheme for any access structure due to its irregular nature. Let a set Γ of subsets of finite set P be the access structure of a secret sharing scheme so that a subset of participants can determine the master key k if and only if that subset is in Γ . It is reasonable to restrict that Γ is monotone. That is,

if $A \in \Gamma$ and $A \subseteq A' \subseteq P$, then $A' \in \Gamma$.

Let 2^P be the power set of P . We define $\partial^+ \Gamma$ to be the family of maximal sets in Γ and $\partial^- \Gamma$ to be the family of minimal sets in Γ , i.e.,

$\partial^+ \Gamma = \{A \in \Gamma \mid A \not\subseteq A' \text{ for all } A' \in \Gamma - \{A\}\}$ and

$\partial^- \Gamma = \{A \in \Gamma \mid A' \not\subseteq A \text{ for all } A' \in \Gamma - \{A\}\}$.

Here, we only consider the access structures that consist of the closure of an access graph where a vertex (edge) represents a participant (a qualified pair of participants). [The closure of a set is the collection of all supersets of the elements of the set.] Note that self-loops may exist in the graph. The self-loop of a vertex u is interpreted as the case that the master key should be reclaimed by the participant u alone. An access structure can be simplified when a self loop exists. Since the access structure must be monotone, if the self-loop for vertex u exists in the access graph, then all vertices must be directly connected to u . In this case, we can delete the vertices with self-loops and their connected edges. The deleted vertices (participants) will be assigned the master key as their shares. Thus, we only need to analyze the new access graph G without self-loops.

Let $V(G)$, $E(G)$ and uv denote the vertex set of G , the edge set of G , and an edge from u to v , respectively. That is,

if uv is an edge of G , then $\{u, v\} \in \partial^- \Gamma$,

if uv is not an edge of G , then $\{u, v\} \in \partial^+ \bar{\Gamma}$ where $\bar{\Gamma} = 2^P - \Gamma$,

if all vertices of G is directly connected to u , then $\{u\} \in \partial^+ \bar{\Gamma}$ where $\bar{\Gamma} = 2^P - \Gamma$.

We will use the conventional threshold scheme and the integer programming technique [11] to construct the perfect secret sharing scheme. The idea is to assign each participant multiple shares in a conventional threshold scheme. Here, we define the *weight* of a participant to be the number of shares kept by him.

Assume $P = \{p_1, p_2, \dots, p_n\}$ and the weight of p_i is w_i , for $1 \leq i \leq n$. We construct the integer programming problem $P(G)$ as follows.

Objection function : $\text{Min } \sum_{i=1}^n w_i$

Subject to :

$$w_i \geq 0,$$

$$w_i + w_j \geq m \text{ if } \{p_i, p_j\} \in \partial^- \Gamma,$$

$$w_i + w_j < m \text{ if } \{p_i, p_j\} \in \partial^+ \bar{\Gamma},$$

$$w_i < m \text{ if } \{p_i\} \in \partial^+ \bar{\Gamma}.$$

When the weights of participants and the value m are determined, we can easily construct a perfect secret sharing scheme by using an $(m, \sum_{i=1}^n w_i)$ threshold scheme

to protect the master key. On one hand, the total number of the shares held by a qualified subset A , $A \in \Gamma$, will be larger than or equal to the threshold value m in the $(m, \sum_{i=1}^n w_i)$ threshold scheme. Hence, the master

key can be reclaimed by A . On the other hand, an unqualified subset B , $B \notin \Gamma$, will obtain no information about the master key because the total number of the shares is less than m . We demonstrate the use of our method in the following example.

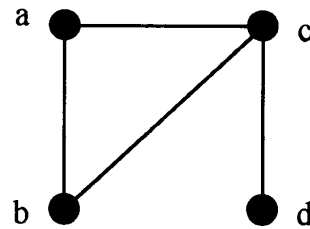


Figure 1. Graph G

In Figure 1, the graph G defines the access structure between members of a set of four participants $P = \{a, b, c, d\}$.

Thus,

$$\Gamma = \{ \{a,b\}, \{a,c\}, \{b,c\}, \{c,d\}, \{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}, \{a,b,c,d\} \}$$

$$\bar{\Gamma} = \{ \{a\}, \{b\}, \{c\}, \{d\}, \{a,d\}, \{b,d\} \}$$

$$\partial^- \Gamma = \{ \{a,b\}, \{a,c\}, \{b,c\}, \{c,d\} \}$$

$$\partial^+ \bar{\Gamma} = \{ \{c\}, \{a,d\}, \{b,d\} \}.$$

Objection function : Min $w_a + w_b + w_c + w_d$

Subject to :

$$w_i \geq 0, \text{ for } i = a, b, c, d.$$

$$w_a + w_b \geq m,$$

$$w_a + w_c \geq m,$$

$$w_b + w_c \geq m,$$

$$w_c + w_d \geq m,$$

$$w_c < m,$$

$$w_a + w_d < m,$$

$$w_b + w_d < m.$$

The optimal solution holds when $w_a = 2, w_b = 2, w_c = 3, w_d = 1$ and $m = 4$. Thus, we can use a (4, 8) threshold scheme to construct the secret sharing scheme for the access structure based on G .

Integer programming technique can be used to construct perfect secret sharing schemes. However, not all integer programming problems have solutions. We will cope with this problem in next section.

3 A construction for special graph-based access structures

Not all integer programming problems have solutions. In this section, we propose a method to overcome the difficulty. Consider the integer programming problem $P(G)$ for the access graph G in Figure 2 (a).

The constraints must contain at least the following four inequalities:

$$(1) \quad w_a + w_c \geq m,$$

$$(2) \quad w_b + w_d \geq m,$$

$$(3) \quad w_a + w_d < m,$$

$$(4) \quad w_b + w_c < m.$$

From (1) and (3), we conclude that $w_c > w_d$. However, from (2) and (4), we conclude that $w_c < w_d$. This is a contradiction. Therefore, the problem $P(G)$ has no solution.

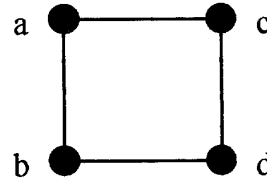


Figure 2 (a) Graph G

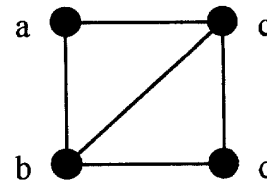


Figure 2 (b) Graph G_a

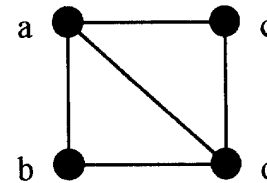


Figure 2 (c) Graph G_b

We will use the concept of composite graphs to overcome the problem. If the integer programming problem $P(G)$ has no solution, we choose graphs G_1, G_2, \dots, G_t in such a way that $G_1 \cap G_2 \cap \dots \cap G_t = G$, and all $P(G_i)$ (for $1 \leq i \leq t$) have solutions. We assume the keys are taken from the finite field $GF(q)$. Let the master key $k = k_1 + k_2 + \dots + k_t \pmod{q}$ where k_i is the sub-master key protected by the perfect sub-secret sharing schemes for the access structures Γ_i based on the graphs G_i . Thus, a secret sharing scheme realizing the access structure of G can be constructed by assigning sub-shares of each sub-secret sharing scheme to each participant. It is clear that if $A \in \Gamma$, then $A \in \Gamma_i$ for $1 \leq i \leq t$. Hence, the qualified subset A of participants can reclaim k_i . Thus, k can be reclaimed. On the other

hand, if unqualified subset $B \notin \Gamma$, then there exists at least one Γ_j (for $1 \leq j \leq t$) such that $B \notin \Gamma_j$. Hence, B obtains no information about k_j . It implies that B also obtains no information about k .

For example, in the Figure 2(a)(b)(c), there is no feasible solution for $P(G)$. Also, $G = G_a \cap G_b$. The solution for $P(G_a)$ is $w_a = 1, w_b = 2, w_c = 2, w_d = 1$ and $m = 3$. And the solution for $P(G_b)$ is $w_a = 2, w_b = 1, w_c = 1, w_d = 2$ and $m = 3$.

For a given graph G with n vertices, the following algorithm can be used to determine generated graphs G_1, G_2, \dots, G_n which have the same vertices as G so that $G_1 \cap G_2 \cap \dots \cap G_n = G$, and all $P(G_i)$ (for $1 \leq i \leq n$) have solutions. We assume that $V(G) = \{p_1, p_2, \dots, p_n\}$. The generated graph G_i can be obtained by the following steps:

- (1) adding a self-loop to p_j ($j \neq i$) if there are $n-1$ edges connecting to p_j in the original G .
- (2) adding edges to connect any two distinct vertices except p_i of the resulting graph in (1).

That is, $V(G_i) = V(G)$ and

$$\begin{aligned} E(G_i) &= E(G) \cup \{uu \mid u \neq p_i, uv \in E(G) \text{ for all } v \in V(G)\} \\ &\quad \cup \{uv \mid u, v \neq p_i, u, v \in V(G), uv \notin E(G)\}. \end{aligned}$$

Theorem 1: The integer programming problem $P(G_i)$ of the generated graph G_i has solution.

Proof: If there exist self-loops in the graph G_i , we only need to consider the problem $P(G_i')$ where G_i' is derived from G_i by deleting the vertices with self-loops and their connected edges. The weights of deleted vertices (participants) are assigned the same value as the threshold value m . So, we only need to consider the case of G_i without self-loops. For the graph G_i ,

$$\begin{aligned} \partial^- \bar{\Gamma}_i &= \{ \{p_i, p_j\} \mid p_i, p_j \in E(G) \text{ for all } j \} \cup \\ &\quad \{ \{p_j, p_i\} \mid 1 \leq j, t \leq n, j \neq t, j, t \neq i \} \text{ and} \\ \partial^+ \bar{\Gamma}_i &= \{ \{p_i, p_j\} \mid p_i, p_j \notin E(G) \text{ for all } j \}. \end{aligned}$$

We assign $m = 2, w_i = 0, w_j = 2$ for all j satisfying $p_i, p_j \in E(G)$ and the other weights are equal 1. Thus, the weight of non-edges of G_i will be less than 2 and the

weight of edges of G_i will be larger than or equal to 2. (Q.E.D.)

Theorem 2: The generated graphs G_1, G_2, \dots, G_n satisfy that $G_1 \cap G_2 \cap \dots \cap G_n = G$.

Proof: It is clear from the construction of G_i that $G \subseteq G_i$ for $1 \leq i \leq n$. So, $G \subseteq G_1 \cap G_2 \cap \dots \cap G_n$. To prove the theorem, we only need to show that $G_1 \cap G_2 \cap \dots \cap G_n \subseteq G$. We will prove it by contradiction. Assume that there exists an edge p_i, p_j (or self-loop) that belongs to $G_1 \cap G_2 \cap \dots \cap G_n$, but not to G . For the construction of graph G_i , p_i, p_j will not be added to the graph G_i because p_i, p_j is connected to p_i . Therefore, $p_i, p_j \notin G_i$. It implies that $p_i, p_j \notin G_1 \cap G_2 \cap \dots \cap G_n$. This is a contradiction to the assumption of $p_i, p_j \in G_1 \cap G_2 \cap \dots \cap G_n$. Hence, $G_1 \cap G_2 \cap \dots \cap G_n \subseteq G$, and thus, $G_1 \cap G_2 \cap \dots \cap G_n = G$. (Q.E.D.)

From *Theorem 1* and *Theorem 2*, we can determine the generated graphs G_1, G_2, \dots, G_n such that $G_1 \cap G_2 \cap \dots \cap G_n = G$, and all $P(G_i)$ (for $1 \leq i \leq n$) have solutions. Thus, the secret sharing scheme can be constructed by combining all sub-secret sharing schemes. It is clear from the proof of the *Theorem 1* that the number of sub-shares held by each participant is at most 2 for each sub-secret sharing scheme, thereby the total number of shares held by each participant is at most $2|\mathcal{P}|$ for the secret sharing scheme. Since the share space can be as large as the master key space in conventional threshold schemes, the information rate of our scheme is at least $1/(2|\mathcal{P}|)$. In contrast, the number of shares held by each participant in the existing scheme is $O(|\mathcal{P}|^2)$ in the worst case [10], and thus the information rate of their scheme is $O(1/|\mathcal{P}|^2)$.

4 Applications

Our secret sharing scheme for graph-based access structures can be employed in many applications in various areas, such as secure communication networks, secure databases. It is particularly useful for access control (e.g., read a file, or send a message) in an environment where the number of participants is large, such as a large secure network. Consider a network system with n participants, where an access control policy is enforced by a key distribution server (KDS) to restrict the communication between participants. A secure session key will not be issued unless the sender requesting the key is allowed to communicate with the

receiver. The access control matrix employed in conventional access control mechanisms can be used by the KDS to achieve the goal [12]. However, the KDS need store and search the large access control matrix of size $O(n^2)$. This size of information causes heavy storage and computation loads on the KDS when n is large. In the worst case, the storage and computation loads may make this design impractical.

In contrast, the perfect secret sharing scheme is more efficient. We can transform the communication relationships into a graph where a vertex denotes a participant and an edge denotes a legal communication. In the network system, each participant holds a shadow (which can be regarded as his private secret key). Two participants present their shadows to the KDS when attempting to communicate. If the two shadows can successfully determine the master key, the KDS will return a session key to both participants. This session key will be used as both encryption and decryption keys for future communication between these two participants. In the scheme, the KDS need not maintain a large access control matrix, but only needs to keep a single master key.

5 Conclusions

In this paper, we propose an efficient construction of perfect secret sharing schemes for graph-based access structures. In contrast to $O(1/|P|^2)$ of existing schemes, the information rate of our scheme is at least $1/2|P|$. Our efficient scheme is useful for access control in an environment where the number of participants is large, such as a large secure network. The KDS based on our scheme need not maintain a large $n \times n$ access control matrix, but only needs to keep a single master key. Thus, the storage and computation loads on the KDS are greatly reduced.

References

- [1] G. R. Blakley, "Safeguarding cryptographic keys," *Proc. AFIPs 1979 National Computer Conference*, New York, Vol. 48, pp. 313-317, 1979.
- [2] A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, no. 11, pp. 612-613, 1979.
- [3] M. Ito, A. Saito and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Proc. IEEE Globecom'87*, Tokyo, 1987, pp. 99-102.
- [4] D. E. R. Denning, *Cryptography and Data Security*, Reading, Addison-Wesley, MA, 1983.
- [5] R. W. Hamming, *Coding and Information Theory*, Englewood Cliffs, Reading, NJ:Prentice-Hall, 1986.
- [6] C. E. Shannon, "Communication theory of secrecy systems," *Computer Security Journal*, Vol. VI, no. 2, pp. 7-66, 1990.
- [7] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," *Advances in Cryptology-Crypto'88 Proceedings*, Lecture Notes in Computer Science, Vol. 403, Springer-Verlag, Berlin, 1990, pp. 27-35.
- [8] E. F. Brickell and D. R. Stinson, "Some improved bounds on the information rate of perfect secret sharing schemes," *Journal of Cryptology*, Vol 5, pp. 153-166, 1992.
- [9] R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, "On the size of shares for secret sharing schemes," *Advances in Cryptology-Crypto'91 Proceedings*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1992, pp. 101-113.
- [10] M. Ito, A. Saito and T. Nishizeki, "Multiple assignment scheme for sharing secret," *Journal of Cryptology*, Vol 6, pp. 15-20, 1993.
- [11] S. Walukiewicz, *Integer Programming*, Kluwer Academic Publishers, 1991.
- [12] B. W. Lampson, "Protection," *Proc. 5th Princeton Symp. of Info. Sci. and Syst.*, Princeton Univ., Mar. 1971, pp. 437-443. Reprinted in *ACM Oper. Syst. Rev.*, Vol. 8(1) pp. 18-24, Jan. 1874.