SUM GRAPH BASED ACCESS STRUCTURE IN A SECRET SHARING SCHEME

SURJADI SLAMET [1], KIKI ARIYANTI SUGENG [1,2] , MIRKA MILLER [2]

Abstract. *Secret sharing scheme* is a method to distribute secret information to a set P of participants so that only authorised subsets of P can reconstruct the secret. A set of subsets of P that can reconstruct the secret is called an *access structure* of the scheme.

A simple undirected graph G is called a *sum graph* if there exists a labeling L of the vertices of G into distinct numbers, usually positive integers, such that any two distinct vertices u and v of G are adjacent if and only if there is a vertex w whose label is $L(w) = L(u) + L(v)$.

In this paper, we will show how sum labeling can be used for representing the graphs of the access structures of a secret sharing scheme. We will combine a known secret sharing scheme such as the classical Shamir scheme with a graph access structure represented using sum graph labeling to obtain a new secret sharing scheme.

Key words : secret sharing scheme, sum graph labeling.
AMS SUBJECT: 94A62

1. Introduction

A *secret sharing scheme* is a method to distribute a piece of secret key or some other secret information, for example, a password or a cryptographic key, to several participants in such a way that only the authorised subsets of participants can access the secret. The family of all authorised subsets of participants is called an *access structure*. A secret sharing scheme is called *perfect* if it is not possible for an unauthorised subset of participants to obtain any information about the secret.

_____

[1] Department of Mathematics, University of Indonesia, Indonesia,
E-mail: slametsis@yahoo.com., kikiariyanti@yahoo.com.
[2] School of Information Technology and Mathematical Sciences, University of Ballarat, Australia, E-mail: m.miller@ballarat.edu.au.

The idea of a secret sharing scheme was first introduced independently by Shamir [6] and Blackley [2], both in 1979. Shamir called his secret sharing scheme a threshold scheme. The piece of information held by each participant was originally called a "shadow" but now it is more usual to call this a "share". A (t, n)- *threshold scheme* is a scheme such that every t participants of a set of n participants can reconstruct or access the secret. However, by combining any $(t - 1)$ or fewer shares, participants cannot gain any information about the secret. To provide greater flexibility, Ito *et al.* [5] generalised Shamir's scheme so that the scheme can be used for general access structures. In such a structure each participant can have more than one share. Ito et al. proved that for every access structure there does exist a secret sharing scheme realising that structure.

The information rate of a secret sharing scheme is the ratio between the number of bits needed to express the secret key and the overall maximum number of bits needed to express each share. Information rate is usually used to measure the efficiency of a system. The symbol that is used for information rate is ρ. Thus

$$\rho = \frac{the \ size \ of \ the \ secret \ in \ bits}{max(the \ size \ of \ a \ share \ in \ bits)}$$

The size of the shares cannot be less than the size of the secret. This property holds since an authorised subsets of participants have absolutely no information about the secret. Csirmaz [4] has proved that for any perfect secret sharing scheme, all participants must have a share at least as the secret itself. A secret sharing schemes is called *an ideal secret sharing scheme* if the information rate for the scheme is 1, i.e., if each share contains as much information as the secret itself.

Many mathematical structures are used to create secret sharing schemes. For example, Brickell and Davenport [3] generated an ideal secret sharing scheme based on matroid theory. Stinson [8] used Brickell and Davenport's scheme to propose a secret sharing scheme based on a graph-based access structure. Subsequently, many researchers tried to find better schemes based on graph access structures.

In this paper we show that sum graph labeling can be used to construct a secret sharing scheme based on a graph access structure. Summable graph labelings will be used for representing the access structure. The construction of secret sharing scheme itself will be built based on the well-known Shamir's threshold scheme.

In this paper we use Shamir's threshold scheme but note that it is not the only possibility, other schemes could be constructed using various secret sharing schemes or threshold schemes.

This paper is organised as follows. Graph based access structures are discussed in Section 2, while Section 3 gives an overview of sum graph labeling.

In Section 4 we construct a secret sharing scheme using sum graph labeling. In Section 5 we give an overview of exclusive sum labeling and construct secret sharing scheme using an exclusive sum labeling.

2. **Sum graph labeling**

A simple undirected graph G is called a *sum graph* if there exists a labeling L of the vertices of G into distinct positive integers such that any two distinct vertices u and v of G are adjacent if and only if there is a vertex w whose label $L(w) = L(u) + L(v)$. The *sum number* $\sigma(H)$ of a (not necessary connected) graph H is the least number r of isolated vertices I_r such that $G = H \cup I_r$ is a sum graph.

In Fig.1 we can see the example of sum labeling for a graph H. We can see that if v and w are the vertices in H then an edge (v, w) is in the graph if and only if $L(v) + L(w)$ is in $H \cup I_r$. For this example, $H = \{1, 2, 3, 4, 5\}$, $I_1 = \{6\}$ and $\sigma(H) = 1$.
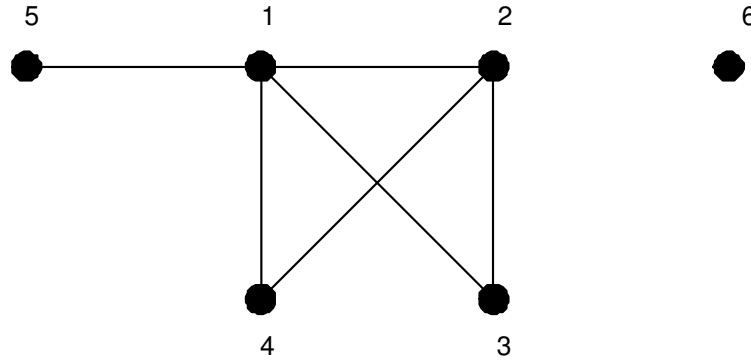

FIGURE 1. An example of a sum graph labeling.

There were many classes of graph that the sum number was known, such an example the sum number of complete graph [1].

3. **Sum labeling on secret sharing scheme**

An access structure of a secret sharing scheme in which every element has an equal size, say m, is called a *uniform access structure of rank m*. Thus, a graph based access structure can be considered as a uniform access structure of rank 2.

Suppose that $G = (V, E)$ is a graph with a set of vertices V and a set of edges E with minimum degree δ and maximum degree Δ. Stinson in [8] proved

that there exists a perfect secret sharing scheme with information rate

$$\rho = \frac{2}{\delta + 1}.$$

Let $P = P_1, P_2, ..., P_n$ be a set of participants from a graph-based access structure of a secret sharing scheme. Then a pair of participants that can access the secret is represented by two adjacent vertices. If we use Shamir's threshold secret sharing scheme for the set P of participants then any two participants can always access the secret. Since usually not every pair of participants allows access to the secret, we combine Shamir's scheme with sum graph labeling for the graph that represents the secret sharing scheme's access structure.

Let $K = (K_1, K_2)$, with $K_1 \neq 0$, be a secret. Let $f(x) = K_1 x + K_2$. Let H be a graph with $V(H) = P = \{P_1, P_2, ..., P_n\}$ and label the vertices in $V(H)$ with sum labeling L. Let I_r be a set of isolated vertices. Let (P_i, P_j) be in $E(H)$ if and only if $L(P_i) + L(P_j) \in H \cup I_r$. A pair of participants (P_i, P_j) can access the secret if and only if (P_i, P_j) is in $E(G)$. Then we have a graph representing the access structure of the secret sharing scheme. A share is given to a participant P_i as follows.

$$S(P_i) = (L(P_i), x(P_i), f(x(P_i))).$$

The key can be recovered by

$$K_1 = \frac{f(x(P_i)) - f(x(P_j))}{x(P_i) - x(P_j)} \chi_{H \cup I_r}(P_i, P_j)$$

and

$$K_2 = f(x(P_i)) - K_2 * x(P_i),$$

where

$$\chi_{H \cup I_r}(P_i, P_j) = 1, \quad \text{if } L(P_i) + L(P_j) \in H \cup I_r$$

and

$$\chi_{H \cup I_r}(P_i, P_j) = 0 \quad \text{if } L(P_i) + L(P_j) \notin H \cup I_r.$$

Suppose that $(P_q, P_r) \notin E(G)$. This means that a pair of participants (P_q, P_r) cannot access the secret. We can see that even if we know the shares of P_q and P_r, we cannot deduce K_1 value, since $\chi_{H \cup I_r}(P_i, P_j) = 0$ and we will have $K_1 = 0$.

Suppose that all the numbers are represented in the same block length bits then since the number of bits needed by K is 2 blocks and every share needs 3 blocks, then the information rate for this structure is $\rho = 2/3$.

From the above discussion, we proved the following theorem.

Theorem 1. Let $P = \{P_1, P_2, ..., P_n\}$ be a set of participants. Let H, with $V(H) = \{P_1, P_2, ..., P_n\}$, be a graph that has a sum graph labeling. Then we

can construct a perfect secret sharing scheme that has a graph-based access structure H. Information rate for this construction is 2/3. $\square$

The next example will give a clear overview of the construction. Let $P = \{A, B, C, D, E\}$. We use Fig. 1. to represents a graph-based access structure.

Let $K = (K_1, K_2) = (2, 5)$ be a key of a secret sharing scheme and $f(x) = K_1 * x + K_2 = 2 * x + 5$. Let $H = \{1, 2, 3, 4, 5\}$ and $I_1 = \{6\}$ so that $H \cup I_r = \{1, 2, 3, 4, 5, 6\}$.

Suppose that we give following shares to participants A, B, C, D and E. Share(A) = (1,1,7), share(B)=(2,2,9), share(C)=(3,3,11), share(D)=(4,4,13) and share(E)=(5,5,15). Thus, if a pair of participants (A, B), with an edge between A and B, want to access the secret, we can get the values of $K_1 = \frac{9-7}{2-1} * \chi_I(A, B) = 2$ and $K_2 = 7 - K_1 = 7 - 2 = 5$.

However, if there is no edge between a pair of participants C and D, then they cannot reconstruct the secret since, if we put the value of the shares of C and D, we only have $K_1 = 0$. Note that we define $K_1 \neq 0$. The information rate for this structure is 2/3.

4. Exclusive graph labeling

In a sum graph G, a vertex w is said to *label* an edge (u, v) if and only if $L(w) = L(u) + L(v)$. The *multiplicity* of w, denoted by $\mu(w)$, is defined to be the number of edges which are labelled by w. If $\mu(w) \geq 0$, then w is called a *working vertex*. If $G = H \cup I_r$ and H contains no working vertices, then H is said to be *exclusive*; otherwise, H is said to be *inclusive*. The labeling L is called *an exclusive labeling* of H if the vertices of H are labeled in a way such that $G = H \cup I_r$ is an exclusive graph. The *exclusive sum number* $\epsilon(H)$ of a graph is the least number r of isolated vertices in I_r such that $G = H \cup I_r$ is a sum graph and H labelled exclusively with $\epsilon(H) = r$.

In [7], the concept of exclusive labeling is discussed and some results for exclusive labeling are given, including the following theorem.

Theorem 2. For a graph G, $\epsilon(G) \geq \Delta(G)$, where $\Delta(G)$ is the maximum degree of G. $\square$

Note that the exclusive sum number is always greater or equal to the sum number, since an exclusive labeling is also a sum labeling.

Let $K = (K_1, K_2)$, with $K_1 \neq 0$, be a secret. Let $f(x) = K_1 x + K_2$. Let H be a graph with $V(H) = P = \{P_1, P_2, ..., P_n\}$ and label the vertices in $V(H)$ with sum labeling L. Let I_r be a set of isolated vertices. Suppose (P_i, P_j) is in $E(H)$ if and only if $L(P_i) + L(P_j) \in I_r$. A pair of participants (P_i, P_j) can access the secret if and only if (P_i, P_j) is in $E(G)$.

As in the previous section, we can generate a secret sharing construction using exclusive sum labeling. We may have more vertices in the isolated set of vertices in exclusive sum labeling than in a sum labeling. However, we have a

simpler way to check if an edge is in the graph or not. We only check whether the sum of the labels of the end-vertices of the edge is in I_r or not, we do not have to check if the sum is in the set of labels of the vertices in H. Note that Theorem 1 also works with an exclusive sum graph labeling instead of the original sum graph labeling.

Suppose we have a graph representing the access structure of the secret sharing scheme. A share is given to participant P_i as follows.

$$S(P_i) = (L(P_i), x(P_i), f(x(P_i))).$$

The key can be recovered by

$$K_1 = \frac{f(x(P_i)) - f(x(P_j))}{x(P_i) - x(P_j)} \chi_{I_r}(P_i, P_j)$$

and

$$K_2 = f(x(P_i)) - K_2 * x(P_i),$$

where

$$\chi_{I_r}(P_i, P_j) = 1 \ \ \text{if } L(P_i) + L(P_j) \in I_r$$

and

$$\chi_{I_r}(P_i, P_j) = 0 \ \ \text{if } L(P_i) + L(P_j) \notin I_r$$

Suppose that $(P_k, P_l) \notin E(H)$. Then $\chi_{I_r}(P_k, P_l) = 0$. In such a case, even if we know the shares of participants P_k and P_l, we still cannot retrieve the secret.

The next example will give a clear overview of the construction. Let $P = \{A, B, C, D, E\}$. Figure 2 represents a graph-based access structure using exclusive sum labeling.
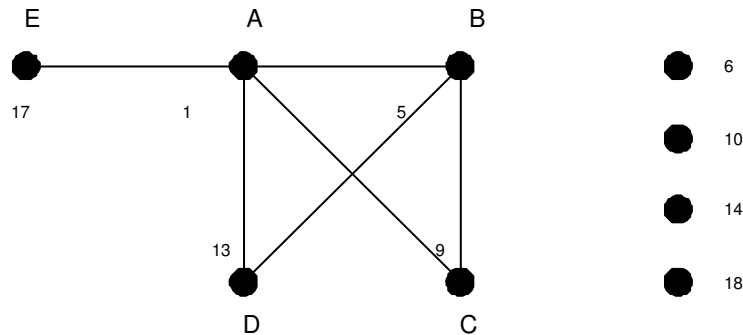

FIGURE 2. An example of a graph-based access structure using exclusive sum labeling.

Let $K = (K_1, K_2) = (2, 5)$ be a key of a secret sharing scheme, the $f(x) = K_1 * x + K_2 = 2 * x + 5$ and $I_r = \{6, 10, 14, 18\}$. Suppose that we give the following shares to participants A, B, C, D and E. Share$(A) = (1,1,7)$, share(B)=(5,2,9), share(C)=(9,3,11), share(D)=(13,4,13) and share (E)=(17,5,15).

Since there is an edge between A and B they can combine their shares to obtain the value of the secret $K = (K_1, K_2)$ where $K_1 = \frac{9-7}{2-1} * \chi_I(A, B) = 2$ and $K_2 = 7 - K_1 = 7 - 2 = 5$. However, since there is no edge between C and D, combining their shares will not recreate the secret but instead will give $K = (0, K_2)$ which is not the secret. The information rate of this structure is also 2/3.

5. **Future work**

The scheme that we presented in this paper uses only a graph-based access structure with rank 2. However, by generalising exclusive graph labeling to exclusive labeling of hypergraphs, it would be also possible to construct a secret sharing scheme for a higher uniform access structure.

REFERENCES

[1] Bergstrand, D., Harary, F., Hodges, K., Jennings, G., Kuklinski, L. and Wiener, J., The sum number of a complete graph, Bull. Malaysian Math. Soc., **12**, (1089), 25-28.

[2] Blackley, G.R., Safeguarding cryptography keys, Proc.AFIPS 1979 National Computer Conference, **48**, (1979), 313-317.

[3] Brickell, E.F. and Davenport, D.M., On the classification of ideal secret sharing schemes, J. of Cryptology, **4**, (1991), 123-134.

[4] Csirmaz, L., The size of a share must be large, Journal of cryptology, **10**, (1007), 223-231.

[5] Ito, M., Saito, A. and Nishizeki, T., Secret sharing scheme realizing general access structure, Proc. IEEE Globecomp, **87**, (1987), 99-102.

[6] Shamir, A., How to share a secret, Communication of the ACM, **22**, (1979), 612-613.

[7] Miller, M., Ryan, J. F., Slamin, Sugeng, K. and Tuga, M., Exclusive sum graph labelings, preprint.

[8] Stinson, D. R., Decompositions construction for secret sharing schemes, IEEE Trans. Inform. Theory, **40**, (1994), 118-125.