Two-level secret sharing schemes based on reverse super edge magic labelings

Md. Shakeel
JNTUH
Hyderabad, Telangana
India

Sharief Basha
VIT Unversity
Vellore, Tamil Nadu
India

Raja Das*
VIT Unversity
Vellore, Tamil Nadu
India
rdasresearch@gmail.com

Abstract. In this paper, we propose two-level secret sharing scheme based on a reverse edge magic labeling of star graphs. It is a scheme which creates two types of hierarchical sets. The first set contains share that are more powerful than the share in the second set. We build banking secret sharing scheme that will share a secret among one bank manager and several sets of authorized staff members.

Keywords: two-level secret sharing schemes, edge-magic total labelling.

1. Introduction

In 1979, Blakley [3], Shamir [7], and Chaum [5] introduced the notion of secret sharing scheme. A secret sharing scheme is a method of allocating a secret S among a finite set of participants $P = \{p_1, p_2, \cdots, p_n\}$ in such a way that if the participants in $A \subseteq P$ are capable to know the secret, then their partial information by pooling together, they can reconstruct the secret S; but any $B \subseteq P$, which is not qualified to know S, cannot reconstruct the secret. The key S which is chosen by a special participant d, called a dealer, and it usually assumed that $d \notin P$. The share means that dealer gives partial information to each participant which is a tool to reveal the secret S. An access structure Γ is the family of all the subsets of participants that are able to reconstruct the secret. The sets belonging to the access structure Γ are called authorized sets and those not belonging to the access structure are termed as unauthorized sets.

A two-level secret sharing scheme is a scheme which produces two kinds of hierarchical sets. The first set (the highest rank) contains shares that are

*. Corresponding author

more powerful (important) than the shares in the second set. In our previous paper, we construct a secret sharing scheme based on reverse edge magic graph labeling. In this paper, we continue our work to plan a two-level secret sharing scheme based on reverse edge magic graph labeling. We provide two different types of such schemes, with two different possible applications.

The first scheme distributes shares of a secret among two sets. The first set (the highest rank set) contains a single person s_0, called a supervisor, and the second set contains a number of chosen people. In the first scheme, the access structure Γ is the family of all sets of the form $\{s_0, p\}$ where p belongs to the second set. We call the first scheme the supervision al secret sharing scheme.

In the proposed second scheme, the first set (the highest rank set) contains a single person s_0. The second set S_2 contains k departments, namely $S_2 = \{D_1, D_2, \cdots, D_k\}$ where each department D_i consists of d_i authorised people. In the second scheme ,the access structure Γ in this second scheme is the family of all sets of the form $\{s_0, x_1, x_2, \cdots, x_k\}$ where $x_i \in D_i$. We name this scheme the departmental secret sharing scheme. These two secret sharing schemes are constructed by reverse edge-magic labeling. The definitions of reverse edge-magic labeling and its related results will be existing in Section II. The proposed schemes will be enlightened in Section III. A conclusion is located in Section IV.

2. Basic theory

In this paper, we considered finite and simple graphs and used general reference for graph-theoretic ideas in [**?**] . The graph G with the vertex-set $V(G)$ and the edge-set $E(G)$ is said to be a reverse edge-magic (REM) labelingthen the one-to-one mapping

$$f : V(G) \cup E(G) \to \{1, 2, 3, \cdots, |V(G) + E(G)|\}$$

satisfying the property that there exists an integer k such that

$$f(xy) - \{f(x) + f(y)\} = k$$

for each edge xy in G. We call $f(xy) - \{f(x) + f(y)\} = k$ the reverse edge difference of edge xy, and k the reverse magic constant of graph G. In particular, if $f(V(G)) = \{1, 2, \cdots, |V(G)|\}$ then f is called reverse super edge-magic labeling. A graph is called reverse(super) edge-magic if it admits any reverse (super) edge-magic labeling.

Venkata Ramana et al [9] introduced and studied the notion of reverse edge-magic graphs with a different name, i.e., graphs with reverse magic valuations, while the term of reverse super edge-magic graphs was firstly introduced by them. They showed that a star $S_{n+1} = K_1$, n is the only complete bipartite graph which is reverse super edge-magic total. They also showed that any odd cycle is reverse super edge-magic, but every wheel is not. Since then, some of authors have studied reverse(super) edge-magic properties in graphs, see, for

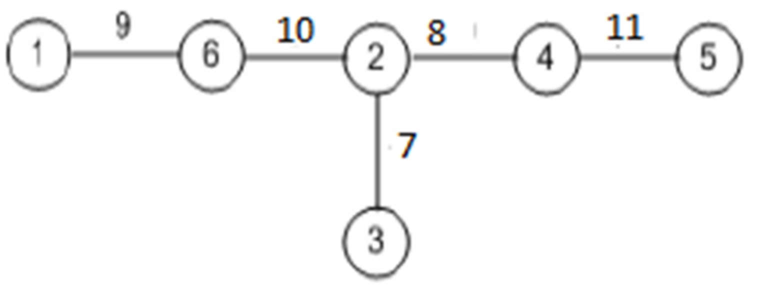

Figure 1: Reverse Super Edge-Magic Labeling

instances, [8, 9]. Figure 1 shows a reverse super edge-magic labeling on graph tree on 6 vertices with the reverse magic constant $k = 2$.

In the following section, we suggest two schemes for secret sharing based on an reverse super edge-magic labeling on a star S_n. The distribution and reconstruction algorithms in this schemes is calculated to work based on our knowledge of reverse super edge-magic labeling, in specific on stars .

3. Proposed schemes

Since the notion of secret sharing scheme introduced, various different types of secret sharing schemes have been proposed (by many authors). They used mathematical structures, such as vector spaces, polynomial, block design, room squares [5], and latin squares [7], to design secret sharing schemes. In this paper, we proposed two schemes for secret sharing based on edge-magic total labeling on graphs.

3.1 Supervisional secret sharing scheme

In supermarkets or banks, when a cashier or teller wants to change or cancel an (important) transaction, on their computer, they will need their supervisor approval to do such a thing. The supervisor will enter a password and then the cashier or teller will complete the entry by his/her own password. In this situation, we can see that the supervisor has more power password then the cashier or teller.

Based on this situation, we build supervisional secret sharing scheme that will share a secret among one supervisor and set of participants under his/her supervision (staffs). In the following we propose an algorithm for this purpose.

Algorithm 3.1

Distribution Algorithm

Input:

- The length of bank manager's share, n_1 (n_1 even).

- The length of bank employee's share, n_2 (n_2 even).
- The number of bank employee, r.

Steps:

1) Build a reverse edge magic labelling on star S_n.
2) Select the label randomly for the center from the integer set $(1, n+1, 2n+1)$, then we have a particular sum k.
3) Compute the labelling.
4) Set k as a secret

Output:

- The share for the bank manager, s_0 (s_0 even).
- The share for each his/her bank employee, p_i for $i = 1, 2, \cdots, r$.

Reconstruction Algorithm
Input:

1) The share of the supervisor, s_0 (s_0 even)
2) The share of one of the staff, L.
3) The size of the star, n (kept by the system)

Steps

1) Built the reverse edge magic number as $H = f(xy) - \{f(x) + f(y)\}$.
2) If H is the reverse edge magic constant k, then the secret is revealed, otherwise secret is not revealed.

Output: The secret is revealed or not.

In this scheme, the secret is an edge-magic total labeling on graph S_n. The secret will be shared to a bank manager and his/her employee.

3.2 Departmental secret sharing scheme

In institutions with several departments, in some situation, to do an agreement, it will need some approval, those are from the head of the institution and faculty from each department. They give their approval by signing the agreement.

Based on this, we build departmental secret sharing scheme that will share a secret among one head of institution and several faculties. These sets represent the departments and the faculties be the authorized representatives.

Algorithm 3.2
Distribution Algorithm (with two departments)
Input:

- The length of share for the director.
- The length of share for each HOD in Department A.
- The length of share for each HOD in Department B.
- The number of Faculties in Department A.
- The number of Faculties in Department B.

Steps:

1) Build a reverse edge magic labelling on Tree $\langle K_{1,n_1}, K_{1,n_2}\rangle$
2) Select , at random, a reverse edge magic labelling k on the Tree $\langle K_{1,n_1}, K_{1,n_2}\rangle$
3) Set λ as a secret.

Output:

- descriptionThe share for the director.
- The share for Faculty in Department A.
- The share for Faculty in Department B.

Reconstruction Algorithm
Input:

The share of Faculty in Department A.

The share of Faculty in Department B.

The share of Director.

The size of a tree

Steps

1) Define $k = f(xy) - \{f(x) + f(y)\}$
2) If $k = \lambda$ then secret is revealed, then otherwise secret is not revealed.

4. Conclusion

This paper proposed two level schemes of secret sharing based on reverse edge-magic labeling on graph G. In these methods, the secret is a chosen reverse edge-magic labeling, in particular, on star S_n and tree $\langle K_{1,n_1}, K_{1,n_2}\rangle$. To distribute the shares, the algorithms work based on a reverse edge magic labeling. The reconstruction algorithms for these schemes are based on our knowledge on k for star/ Tree.

References

[1] E.T. Baskoro, M. Miler Slamin, W.D. Wallis *Edge magic total labelings* , Australasian Journal of Combinatorics, 22 (2000), 177-190.

[2] E.T. Baskoro, R. Simanjuntak, M.T. Adithia, *Secret Sharing scheme based on magic labeling*, Proc. of the 12th National Conference on Mathematics, 2004, 23-27.

[3] G.R. Blakley, *Safeguarding cryptographic keys*, Proc. AFIPS, New York, 48 (1979), 313-317.

[4] G.R. Chaudhry, H. Ghodosi, J. Seberry, *Perfect secret sharing schemes based on room squares.*

[5] D. Chaum, *Computer systems established, maintained, and trusted by mutually suspicious groups*, Memorandum No. UCB/ERL M179/10, University of California Berkeley, CA, 1979.

[6] E.D. Karnin, J.W. Greene, M.E. Hellman, *On Secret Sharing Systems*, IEEE Trans. Inf. Th., vol. IT-29(1), 1983, 35-41.

[7] A. Shamir, *How to Share a Secret*, Comm. ACM, 22 (1979), 612-613.

[8] Md. Shakeel, S. Sharief Basha, K.J. Sarma Smieee K.J., *Algorithms for constructing Reverse edge magic labelling of complete bipartite graphs*, Global Journal of Pure and Applied Mathematics, 12, 707-710.

[9] S. Venkata Ramana, S. Sharief Basha, *Reverse Super edge magic labelling of a graph*, PhD Thesis, 2009.

Accepted: 13.12.2017