Secret Sharing Algorithm based on Reverse Edge-magic Labeling on Graphs and its Application

Sharief Basha S
VIT, Vellore, Tamil Nadu 632014, India

Raja Das
VIT, Vellore, Tamil Nadu 632014, India

Abstract- We investigated the reverse super edge-magic labeling on graphs, especially star, and application on secret sharing algorithm. In this paper we show how to divide 2n+1 data into n pieces in such way that 2n+1 data is easily reconstructable from any n pieces, but even complete knowledge of n pieces discloses absolutely no information about 2n+1 data. This algorithm assists the construction of locker key management for banking system that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

Keywords – Secret Sharing, Cryptography, Key Management, and Reverse edge Magic Labeling

I. INTRODUCTION

Blakley [2], Shamir [6], and Chaum [4] in 1979 first introduced secret sharing schemes. A secret sharing scheme (see [4]) is one type of method of sharing a secret *S* among some set of customers $C = \{C_1, C_2, \cdots, C_n\}$ in such a way that if the customers in *A* *C* are qualified to know the secret, then by pooling together their partial information, they can reconstruct the secret *S*; but any *B* *C*, which is not qualified to know *S*, cannot reconstruct the secret. The key S is selected by special person D, called manager of the bank, and it usually assumed that *D* *C*. The manager gives partial information, called share, to each customer to share the secret *S*.

An access structure is defined the family of all the subsets of customers that are able to reconstruct the secret. The sets of *C* going to the access structure are called authorised sets and those not fitting to the access structure are named as unauthorised sets.

A secret sharing scheme is said to be perfect if an unauthorised subset of customers *B* *C* pool their shares, then no one from outsider can control about the value of secret *S*.

In this paper, we examine the reverse edge-magic labelings on graphs, especially star, which is the application of secret sharing.

The vertex set $V(G)$ and edge set $E(G)$ of a graph G, a reverse edge-magic labeling [7, 8] is a one to one map $\lambda: V(G) \cup E(G)$ to the set of integers $\{1, 2, 3, \cdots |V(G) \cup E(G)|\}$ with the property that there exists an integer k such that

$$\lambda(uv) - \{\lambda(u) - \lambda(v)\} = k$$

for any edge $uv \in E(G)$. We call $\lambda(uv) - \{\lambda(u) - \lambda(v)\}$ the difference between the edge labeled value and the sum of the vertices of that edge labelled values, and k the reverse magic value of graph *G*. A graph is called reverse magic if it admits any edge-magic labeling.

We number all edges and all vertices for each graph, then we call these numbers positions. Thus, a graph labeling can be characterized as a set of well-ordered pairs of position and its label.

II. STAR

Star is one special form of tree, that is a tree with a vertex as center and the all other vertices are leaves. S_n is star with *n* leaves.

Based on [7,8], in Type1 ,all stars is reverse edge-magic with $k = n - 1$ when the center receives label 1,in Type 2, reverse edge-magic constant $k = 0$ when the center receives label $n + 1$, and in Type 3 , the reverse edge-magic constant $k = -(n + 1)$ which is occurred when the center receives label $2n + 1$.

In Type 1, let S_n be a star of $n+1$ vertices where the vertex set. Now in some order, we number all of the vertices by integers $1, 2, \cdots, n+1$ with the center receives number 1. Thus all edges in S_n are of the form $(1, j)$ where$j = 2, 3, \cdots, n+1$. Next we endure numbering the edges as follows,

$1, 2$, numbered with $n+2$

$1, 3$, numbered with $n+3$

$1, 4$, numbered with $n+4$

…

…

…

$1, n+1$, numbered with $2n+1$

Thus we can represent the reverse edge-magic labeling on star as a set of ordered pairs of position and its label.

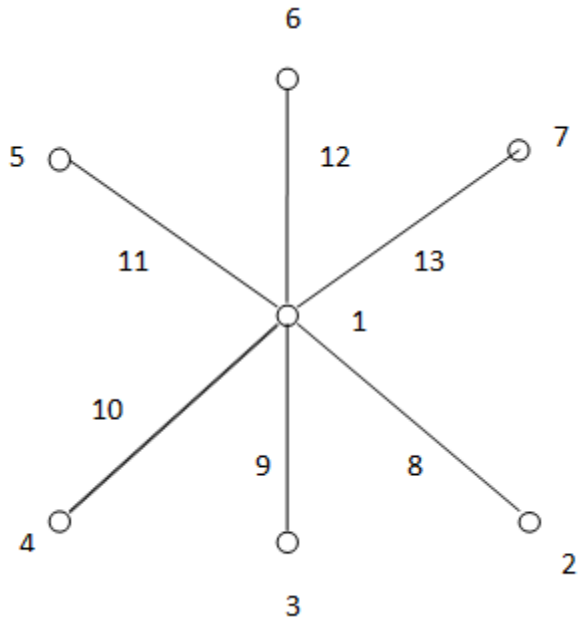

Figure 1. Reverse edge magic labelling of Star graph S_6 as center label 1 & $k = 5$

In Type 2 , Let S_n be a star of $n+1$ vertices where the vertex set . Now in some order, we number all of the vertices by integers $1, 2, 3, \cdots, n+1$ with the center receives number $n+1$. Thus all edges in S_n are of the form $(n+1, j)$, where $j = 1, 2, 3, \cdots, n$. Next we endure numbering the edges as follows,

$n+1, 1$, numbered with $n+2$

$n+1, 2$, numbered with $n+3$

$n+1, 3$, numbered with $n+4$

…

…

…

$n+1, n$, numbered with $2n+1$

Thus we can represent the reverse edge-magic labeling on star as a set of ordered pairs of position and its label.

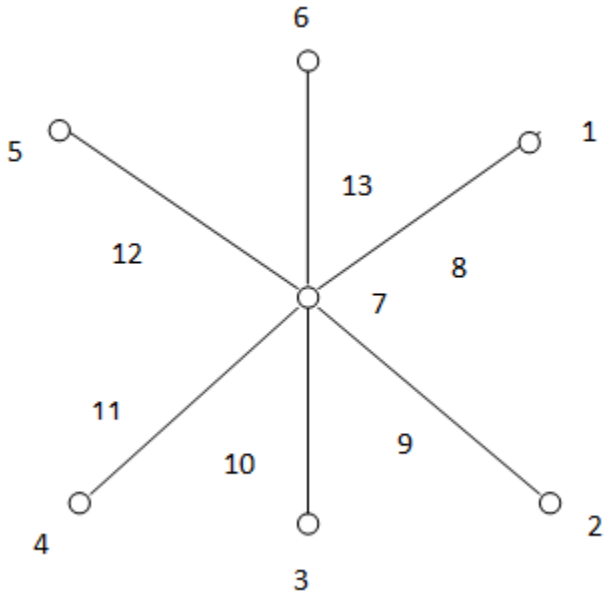

Figure 2. Reverse edge magic labelling of Star graph S_6 as center label 7 & $k = 0$

In Type 3, Let Sn be a star of $n + 1$ vertices where the vertex set. Now in some order, we number all of the vertices by integers $1, 2, 3, \cdots, n + 1$ with the center receives number $2n + 1$. Thus all edges in Sn are of the form $(2n + 1, j)$, where $j = 1, 2, 3, \cdots, n$. Next we endure numbering the edges as follows,

$2n + 1, 2$, numbered with $n + 1$
$2n + 1, 3$, numbered with $n + 2$
$2n + 1, 4$, numbered with $n + 3$
…
…
…
$2n + 1, n$, numbered with $2n$

Thus we can represent the reverse edge-magic labeling on star as a set of ordered pairs of position and its label.

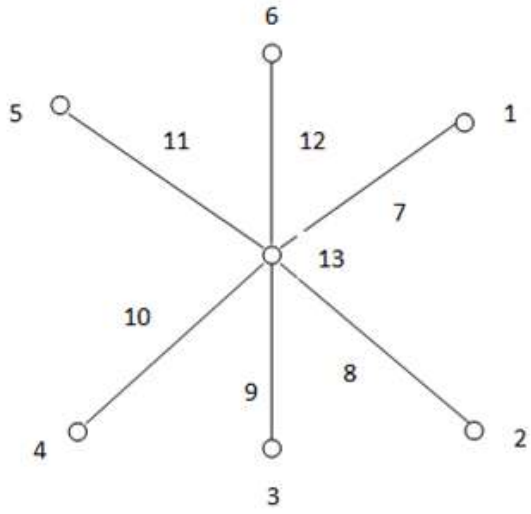

Figure 3. Reverse edge magic labelling of Star graph S_6 as center label 13 & $k = 7$

III. 3. SECRET SHARING SCHEME ALGORITHM

Input

- *n*: size of star.
- *r*: number of customers.

Steps:

1. Build a reverse edge magic labelling on star Sn by using the following method:
   (a) Select the label randomly for the center from the integer set$(1, n+1, 2n+1)$, then we have a particular sum *k*.
   (b) Compute the labelling.
2. Built the reverse edge magic number k from the result on step 1, select the positions along with their labels.
3. Type will be selected.
4. Distribute the shares (OTP) to the corresponding customer's mobile.
5. The locker will be open digitally by reverse edge magic number k.

Output: The shares

IV.CONCLUSION

In this paper, we investigated the various reverse edge magic labelling and its application. We proposed a secret sharing scheme based on reverse edge magic labelling on star graphs with type 1, type 2 and type 3 labeling system. The proposed algorithm helps the digital bank locker key management for banking system. This algorithm can be function securely and reliably.

The direction for future research are:

- Construction of families of reverse edge magic labelling for tree.
- Construction of maximum and minimum reverse super edge magic labelings for tree.
- Quantify the security of secret scheme more effectively by using reverse edge magic labelling assignment of vertices and edges with numbers randomly.
- Devise multilevel schemes based on reverse edge magic labelings.

REFERENCES

[1] E.T. Baskoro, M. Miler, Slamin and W.D. Wallis, Edge Magic Total Labelings .
[2] G.R. Blakley, Safeguarding Cryptographic Keys, Proc. AFIPS 1979, New York, vol. 48, pp. 313-317, 1979.
[3] G.R. Chaudhry, H. Ghodosi , J. Seberry, Perfect Secret Sharing Schemes based on Room Squares.
[4] D. Chaum, Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups, Memorandum No. UCB/ERL M179/10, University of California Berkeley, CA, 1979.
[5] E.D. Karnin, J.W. Greene, and M.E. Hellman, "On Secret Sharing Systems", IEEE Trans. Inf. Th., Vol. IT-29, No. 1, pp. 35-41, 1983.
[6] A. Shamir, How to Share a Secret, Comm. ACM, vol. 22, No. 11, pp.612-613, 1979.
[7] Md.Shakeel, Sharief Basha.s and K.J Sarma Smieee, Algorithms for constructing Reverse edge magic labelling of complete bipartite graphs, Global Journal of Pure and Applied Mathematics, vol. 12, No. 3, pp:707-710, 2016.
[8] S.Venkata Ramana and Sharief Basha.S, Reverse Super edge magic labelling of a graph, PhD Thesis, 2009.