Critical set of caterpillar graph for secret sharing scheme*

Chairul Imron[1], Budi Setiyono[1]
R. Simanjuntak[2], Edy T. Baskoro[2]

[1] Mathematics Department ITS
imron-its@matematika.its.ac.id, mazh_budi@yahoo.com
[2] Mathematics Department ITB
{rino,ebaskoro}@dns.math.itb.ac.id

Abstract. We investigate the critical set of edge-magic labeling on caterpillar graphs and application on secret sharing scheme. We construct a distribution scheme based on supervisional secret sharing scheme. The schemes use the notion of critical sets to distribute the share and reconstruct the key.

Keywords: Caterpillar graph, secret sharing scheme, edge-magic total labeling, critical sets.

1 Introduction

A secret sharing scheme is method of distributing a secret S among a finite set of participants $\mathbb{P} = \{p_1, p_2, \cdots, p_n\}$ in such a way that if the participants in $A \subseteq \mathbb{P}$ are qualified to know the secret, but any $B \subseteq \mathbb{P}$ which is not qualified to know secret. The participant which qualified with pooling together their partial information, they can reconstruct the secret S, but participant not qualified they can not reconstruct the secret. The key S is chosen by special participant d and usually assumed that $d \notin \mathbb{P}$.

A two level secret sharing scheme is a scheme which produces two kinds of hierarchical sets. The first set contains shares that are more powerful than the shares in the second set. The first scheme distributes shares od secret among two sets. The first set containt a single person, called a supervisor, while the second set contains a number of chosen people. The access structure in this first scheme is the family of all sets of the form $\{s_0, p\}$ where p belongs to the second set. We call scheme is the supervisional secret sharing scheme.

2 Basic Theory

In this paper, we investigate the critical sets of edge-magic total labelings on caterpillar graph and the application on secret sharing.

* Supported by Hibah Pekerti Dikti 2006

For a graph $\mathbb{G}$ with the vertex-set $V(\mathbb{G}) = \{v_1, v_2, \cdots, v_p\}$ and the edge-set $E(\mathbb{G}) = \{e_1, e_2, \cdots, e_q\}$ and definition of edge magic total labeling is

Definition 1. *An edge-magic total labeling of a (p,q)-graph $\mathbb{G}$ is bijective function*

$$\lambda : V(\mathbb{G}) \cup E(\mathbb{G}) \rightarrow \{1, 2, 3, \cdots, p+q\}$$

such that

$$\lambda(u) + \lambda(uv) + \lambda(v) = k \tag{1}$$

k is a constant for any edge uv of $\mathbb{G}$ and is called the magic sum of $\mathbb{G}$. Any graph with an edge-magic total labeling will be called edge-magic[11]. Morever, λ is a super-edge-magic total labeling of $\mathbb{G}$ if $\lambda(V(\mathbb{G})) = \{1, 2, 3, \cdots, p\}$, and $\mathbb{G}$ is said to be super-edge-magic[4].

For each graph, we number all vertex and edges, we call these numbers positions. Thus, a graph labeling can be represented as a set of ordered pairs of position and its label.

A critical set of a graph $\mathbb{G}$ with labeling λ is a set $Q_\lambda = \{(x, y) | x, y \in \{1, 2, \cdots, |V(\mathbb{G}) + E(\mathbb{G})|\}$, with the oredered pair (x, y) represents label y in position x, which satisfy[3]

1. λ is the only labeling of $\mathbb{G}$ which has label y in position x
2. No proper subset of Q_λ

If cardinality of a critical set is c, thus it has size c. A critical set $Q_{\lambda i}$ has minimal size, if $|Q_{\lambda i}| \leq |Q_{\lambda j}|$

3 Caterpillar Graph

Caterpillar is one special form of tree, which is a tree with some vertices as center and all other vertices are leaves, or we called n stars. Consider caterpillar graph C_n with $V = \{S_1, S_2, \ldots, S_n\}$ where $S_i = \{v_{i0}, v_{i1}, v_{i2}, \ldots, v_{ip_1}\}$ dan p_i is sum of leaf at S_i and v_{i0} is center vertex star i, where $i = 1, 2, \cdots, n$. Sum of vertices caterpillar graph C_n are sum of all leaf at star plus center vertex of star or

$$v = \sum_{i=1}^{n} |S_i| = \sum_{i=1}^{n} (p_i + 1) = n + \sum_{i=1}^{n} p_i$$

and sum of edge caterpillar graph C_n is $e = v - 1$ such that integer number need for labeling is

$$v + e = 2(n + \sum_{i=1}^{n} p_i) - 1$$

All caterpillars is edge-magic total labeling with some method labeling [6, 12], like Figure 1.

Position label of vertices and edges, begin center of first star, edge and then leaf and so on, such that we have edge-magic total labeling with position is

$$\lambda = \{(1, k+1), (2, v+e), (3, 1), (4, v+e-1), \cdots, (v+e, v)\}$$

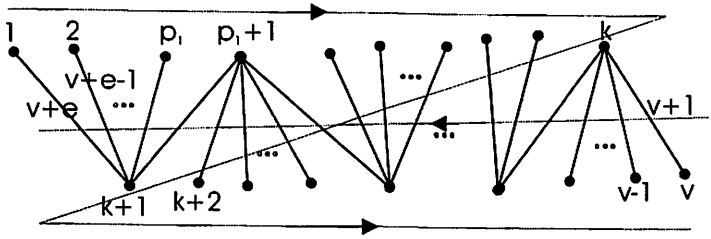

Fig. 1. EMTL of Caterpillar Graph

If Q is critical set and minimal number of critical set in caterpillar graph C_n is the number of leaf, then [10]

$$|Q(C_n)| = \sum_{i=1}^{n} p_i$$

note by that set is containt the label in the leaf, edge of leaf or both of them. The label which in critical set is not containt all big number or small number, but both of them.

The example caterpillar graph C_3 in Figure 2 with edge-magic total labeling

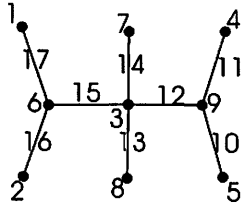

Fig. 2. EMTL of C_3

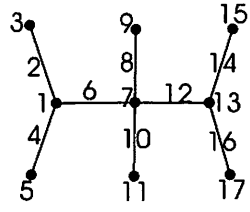

Fig. 3. Position of C_3

so the posibility of edge-magic total labeling are

$\lambda_1 = \{(1,6),\mathbf{(2,17)},\mathbf{(3,1)},(4,16),(5,2),(6,15),(7,3),(8,14),(9,7),(10,13),$
$(11,8),(12,12),(13,9),(14,11),(15,4),(16,10),(17,5)\}$

$\lambda_2 = \{(1,6),\mathbf{(2,1)},\mathbf{(3,17)},(4,16),(5,2),(6,15),(7,3),(8,14),(9,7),(10,13),$
$(11,8),(12,12),(13,9),(14,11),(15,4),(16,10),(17,5)\}$

and critical set from that both edge-magic total labeling are

$Q_{\lambda_1} = \{\mathbf{(2,17)},(4,16),(8,14),(10,13),(14,11),(16,10)\}$

$Q_{\lambda_2} = \{\mathbf{(2,1)},(4,16),(8,14),(10,13),(14,11),(16,10)\}$

obviously after reconstruction, Q_{λ_1} have more than one edge-magic total labeling, which are

$$\begin{aligned}\lambda_{11} &= \{(1,6),\mathbf{(2,17)},\mathbf{(3,1)},(4,16),(5,2),(6,15),(7,3),(8,14),(9,7),(10,13),\\ &\quad (11,8),(12,12),(13,9),(14,11),(15,4),(16,10),(17,5)\}\\ \lambda_{12} &= \{(1,1),\mathbf{(2,17)},\mathbf{(3,6)},(4,16),(5,7),(6,15),(7,8),(8,14),(9,2),(10,13),\\ &\quad (11,3),(12,12),(13,9),(14,11),(15,4),(16,10),(17,5)\}\end{aligned}$$

so Q_{λ_1} is not critical set because the reconstruction is not unik. The criticalset which used for scheme are

$$\begin{aligned}Q_1 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,13),(14,11),(16,10)\}\\ Q_2 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,13),(14,11),(16,5)\}\\ Q_3 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,13),(14,4),(16,10)\}\\ Q_4 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,13),(14,4),(16,5)\}\\ Q_5 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,8),(14,11),(16,10)\}\\ Q_6 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,8),(14,11),(16,5)\}\\ Q_7 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,8),(14,4),(16,10)\}\\ Q_8 &= \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)},(10,8),(14,4),(16,5)\}\end{aligned}$$

4 Proposed Schemes

In supermarket, when a cashier wants to changes or cancel an transaction, they will need supervisor approval to do such a thing. The supervisor will enter a password and then the casier 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. Based on situation, we build secret sharing scheme that will share a secret among one supervisor and set of participants under supervision stafs.

¿From the critical set that built above, we can make a secret for supervisor, which is

$$S = \bigcap_{i=1}^{n} Q_i = \{\mathbf{(2,1)},\mathbf{(4,16)},\mathbf{(8,14)}\}$$

and the eight secret for staff, which are

$$\begin{aligned}P_1 &= \{(10,13),(14,11),(16,10)\}\\ P_2 &= \{(10,13),(14,11),(16,5)\}\\ P_3 &= \{(10,13),(14,4),(16,10)\}\\ P_4 &= \{(10,13),(14,4),(16,5)\}\\ P_5 &= \{(10,8),(14,11),(16,10)\}\\ P_6 &= \{(10,8),(14,11),(16,5)\}\\ P_7 &= \{(10,8),(14,4),(16,10)\}\\ P_8 &= \{(10,8),(14,4),(16,5)\}\end{aligned}$$

If a participant (for example P_4) and supervisor (S) want to know the secret (is qualified or not), they must to pooling together

$$\begin{aligned} P_4 \cup S &= \{(10,13),(14,4),(16,5)\} \cup \{(2,1),(4,16),(8,14)\} \\ &= \{(2,1),(4,16),(8,14),(10,13),(14,4),(16,5)\} \\ &= Q_4 \end{aligned}$$

5 Conclusions

This paper proposed secret sharing scheme based on edge-magic total labeling on graph, specially caterpillar graph. From edge-magic total labeling, we founded some critical set and then to distribute to some participants and one supervisor. If we want know secret of supervisor or participant is qualified or not, they must to pooling together.

References

1. M.T. Adithia *Himpunan kritis suatu pelabelan graph*, Tesis, 2000.
2. E.T. Baskoro, Critical Sets in Edge-Magic Total Labelings. 2005.
3. E.T. Baskoro, Secret Sharing Scheme Based on Magic Labeling , Proc. of the 12^{th} National Conference on Mathematics, Bali, 23-27 July, 2004.
4. Enomoto, H., A.S. Llado, T. Nakamigawa and G. Ringel, 1998), *Super Edge-Magic Graphs*, SUT Jurnal of Mathematics, Vol. 34, No. 2, 105-109.
5. Chairul Imron, Variasi Pelabelan Graph Lintasan dan Star, Seminar Nasional Matematika ITS, 4 Desember 2004.
6. Chairul Imron, Several Ways to Obtain Edge-Magic Total Labelings of Caterpillars, International Workshop on Graph Labeling, Batu, Malang, 6-9 Desember 2004.
7. Variasi Pelabelan Graph Lintasan dan Star, Seminar Nasional Matematika di Jurusan Matematika FMIPA ITS Surabaya, 2004.
8. Pelabelan Total Sisi-Ajaib Graph Caterpillar, Seminar Nasional Matematika di Universitas Negeri Surabaya, 28 Februari 2005.
9. Magic Graph on Cycle, The First International Conference on Mathematics and Statistics, UNISBA, Bandung, 19-21 Juni 2006. 13. Himpunan Kritis Graf Caterpillar, Konferensi Nasional Matematika XIII, UNNES, Semarang, 24-27 Juli 2006.
10. Chairul Imron, Budi Setiyono, R. Simanjuntak, Edy T. Baskoro, Himpunan Kritis pada Graph Caterpillar, Konferensi Nasional Matematika XIII (Proseding), UNNES Semarang, 24-27 Juli 2006.
11. Wallis, W.D., E.T. Baskoro, M.Miller and Slamin, (2000), *Edge-Magic Total Labelings*, Australian Journal of Combinatorics 22, 177-190.
12. A. Kotzig and A. Rosa: Magic Valuation of Finite Graphs, Canad. Math. Bull 13 (1970) 451-461.