Minimax Theory and its Applications

Volume 11 (2026), No. 3s, 853 to 867

A Dominating Edge Block Partition Framework for Graph-Access Secret Sharing

Sreenivasulu Reddy L[1], Nimmy Chacko[2]

[1]Associate Professor Department of Mathematics, School of Advanced Sciences, Kalasalingam Academy of Research and Education (Deemed to be University), Krishnankoil, 626126, Tamilnadu, India.
Email: sreenivasulureddy.svu@gmail.com, Orcid id: https://orcid.org/0000-0002-7396-8026
[2]Research scholar, Department of Mathematics, School of Advanced Sciences, Kalasalingam Academy of Research and Education (Deemed to be University), Krishnankoil, 626126, Tamilnadu, India.
Email: nimmichan87@gmail.com, Orcid id: 0009-0003-8785-0373

Abstract
Participant relationships can direct share distribution and secret reconstruction in graph-access secret sharing systems, where the access structure is determined by the structural characteristics of an underlying graph. The Dominating Edge Block Partition (DEBP), a graph-theoretic technique for creating graph-access secret sharing methodsin which the selected dominating vertices collectively constitute the authorized participant set, is introduced in this study. The suggested DEBP operator divides the edge set of a connected graph with one of its dominating sets into pairwise disjoint connected edge blocks, each of which is uniquely connected to a dominating vertex. The dealer distributes these block shares according to the graph access structure generated by the dominating set, represents the secret as the sum of edge labels, and calculates one block share for each dominating vertex by aggregating the labels of the corresponding edge block. The permitted dominating vertices' block shares are combined to accomplish secret reconstruction.
The suggested framework introduces the use of graph-theoretic operations in cryptography by establishing a direct relationship between graph domination, edge splitting, and secret sharing. Formal mathematical proofs confirm the construction's correctness, and once the dominating set has been identified, its computational complexity is demonstrated to be linear in the number of graph edges. Detailed constructions on path graphs, cycle graphs, complete binary trees and grid graphs illustrate the applicability of the suggested framework. The suggested DEBP framework gives a platform for future studies on graph-theoretic techniques in safe information distribution as well as a methodical way for creating graph-access secret sharing schemes.

Keywords: Graph-access secret sharing, Dominating set, Dominating Edge Block Partition (DEBP), Edge partition, Access structure, Graph theory, Connected graphs, Share distribution, Cryptography.

1. Introduction

By dividing a secret among several participants so that only authorized subsets may reassemble the original secret, secret sharing is a basic cryptographic approach for safeguarding sensitive data. Threshold secret sharing was first introduced by Shamir [1] and Blakley [2], whose groundbreaking techniques laid the theoretical groundwork for later advancements. This idea was further expanded upon by Ito, Saito, and Nishizeki, who introduced secret sharing techniques that enable authorization rules beyond threshold-based reconstruction by realizing arbitrary access structures [3], [4]. Karnin et al. [5], Brickell [6], Blundo et al. [7], Stinson [8], [9], and Benaloh and Leichter [11] later made a number of improvements in terms of information rate, share size, and building methodologies.

Because graphs offer a natural representation of participant interactions, graph theory has become more and more significant in the study of secret sharing. Participants are represented as vertices in graph-access secret sharing methods, and the permitted subsets are determined by graph-theoretic features. Existing studies have investigated graph access structures based on graph connectivity, independent sets, vertex covers, cliques, bipartite graphs, and forbidden graph structures [21] – [26].Specifically, a polynomial-time decomposition approach for graph access structures was proposed by Sun et al. [21], and the efficiency and complexity of secret sharing schemes related to graph-based access structures were examined by Csirmaz [22] and Beimel et al. [23]–[25]. These contributions show how well graph-theoretic methods work for creating adaptable permission systems.

A number of mathematical ideas from general graph theory are pertinent to the safe dissemination of information. The theoretical underpinnings for graph representations, connectivity, graph decomposition, and distance measurements utilized in graph-based cryptographic constructions are provided by standard graph-theoretic references by Harary [12], Bondy and Murty [13], Deo [14], West [15], Bollobás [16], and Diestel [17].

Domination has drawn a lot of attention among different graph metrics because dominant vertices effectively convey a graph's influence or coverage. Cockayne and Hedetniemi [18] laid the theoretical groundwork for dominance, which Haynes, Hedetniemi, and Slater [19], [20] expanded upon in their extensive monographs. Because dominating sets offer compact representative subsets of graph vertices, they have been extensively used in communication networks, wireless sensor networks, routing, facility locating, and distributed systems.

According to recent studies, graph theory is still becoming more and more important in the study of secret sharing. A thorough analysis of contemporary secret sharing schemes, including threshold, hierarchical, multi-secret, and verified secret sharing, as well as new research avenues, was provided by Chattopadhyay et al. [27]. In a similar vein, Drissi and Akdim [28] examined graph-theoretic applications in secret sharing and discussed about the use of combinatorial techniques, graph access structures, and graph deconstruction for safe information transfer. The computational elements of secret sharing, graph access architectures, and information complexity have been further examined in more recent studies [24], [25], and [29], indicating the ongoing interest in graph-based cryptography approaches.

The integration of graph deconstruction and domination into a unified graph-access secret sharing structure received very little attention, despite the fact that both have been thoroughly investigated. This insight serves as the inspiration for this paper's Dominating Edge Block Partition (DEBP) framework, which divides a linked graph's edge set into pairwise disjoint edge blocks connected to a chosen dominating set. The resulting partition, which offers a systematic approach for share generation and secret reconstruction, serves as the foundation for the suggested graph-access secret sharing scheme.

The following is a summary of this work's main contributions.

1. To divide a connected graph's edge set according to a chosen dominating set, a graph-theoretic framework known as the Dominating Edge Block Partition (DEBP) is put forth.
2. A deterministic approach for creating linked edge partitions based on domination is introduced.
3. Based on the DEBP structure, a framework for graph-access secret sharing is created.
4. The suggested framework is established using formal mathematical definitions, methods, and correctness proofs.
5. The DEBP construction's computational complexity and the related secret sharing processes are examined.
6. Detailed examples involving path graphs, cycle graphs, complete binary trees and grid graphs, demonstrate the applicability of the suggested model.

The suggested DEBP system integrates edge splitting and graph domination into a single method for graph-access secret sharing. It offers a systematic method to building edge-based share distributions and lays the groundwork for future research into graph-theoretic methods in safe information sharing and associated cryptography applications.

2. Preliminaries

Let $G = (V, E)$ represent a finite, simple, connected, undirected graph for the purposes of this work, where $V = \{v_1, v_2, \ldots, v_n\}$ is the vertex set and $E = \{e_1, e_2, \ldots, e_m\}$ is the edge set.

The number of vertices is represented by the symbol $n = |V|$ and $m = |E|$ represent the number of vertices and edges, respectively.

Definition 2.1 (Dominating Set)

If every vertex $v \in V \setminus D$ is adjacent to at least one vertex in D then the subset $D \subseteq V$ is referred to as a dominant set of G.

Formally, $\forall v \in V \setminus D, \exists d \in D$ such that $(v, d) \in E$.

Definition 2.2 (Minimum Dominating Set)

A minimum dominating set is a dominating set with the smallest cardinality.The dominance number, represented by γ(G), represents its size.

Definition 2.3 (Edge Partition)

An edge partition of a graph $G = (V, E)$is a family $\mathscr{B} = \{B_1, B_2, \dots, B_k\}$such that $B_i \subseteq E$, satisfying $B_i \cap B_j = \emptyset, i \neq j$,and $\bigcup_{i=1}^{k} B_i = E$.As a result, each edge is a part of a single block.

Definition 2.4 (Connected Edge Block)

An edge block $B_i$is called **connected** if the subgraph $G[B_i]$induced by its edges isconnected.

Definition 2.5 (Graph Access Structure)

Let the participants be $P = \{P_1, P_2, \dots, P_n\}$. A family $\Gamma \subseteq 2^P$that has every member of Γ approved and every superset of an authorized set authorized is called a graph access structure.

3. Dominating Edge Block Partition (DEBP)

The Dominating Edge Block Partition (DEBP), which is the main theoretical contribution of this study, is introduced in this section. DEBP is a graph operator that converts a connected graph and one of its dominating sets into a group of connected edge blocks, in contrast to traditional edge partitioning methods. The share distribution in the suggested graph access secret sharing system is then determined by these edge blocks.

Definition 3.1 (Dominating Edge Block Partition Operator)

Let $G = (V, E)$be a connected graph and let $D = \{d_1, d_2, \dots, d_k\}$be a dominating set of G.

The Dominating Edge Block Partition Operator (DEBP) is the mapping

$\mathcal{D}: (G, D) \rightarrow \{B_1, B_2, \dots, B_k\}$

where $B_i \subseteq E$,satisfying the following axioms.

Axiom 1 (Edge Coverage)

Each edge is a part of a block.

$$\bigcup_{i=1}^{k} B_i = E$$

Consequently, no edge is left out.

Axiom 2 (Disjointness)

For $i \neq j, B_i \cap B_j = \emptyset$

Therefore, every edge is a part of a single block.

Axiom 3 (Dominating Association)

Every block $B_i$is exclusively connected to the dominating vertex d_i.

Consequently, $B_i \leftrightarrow d_i$.

There is a one-to-one relationship.

Axiom 4 (Connectivity)

The subgraph that $B_i$inducesis connected.As a result, each block serves as a single connected component for the computation of shares.

Axiom 5 (Maximality)

In terms of connectedness, every block is maximal without going against Axioms 1-4.

This indicates that $B_i$cannot have any further edges added to it without disconnecting or overlapping another block.

4. Deterministic Edge Assignment and Dominating Set Selection

Let$G = (V, E)$be a graph that is connected. A selected dominating set of G is used to define the suggested Dominating Edge Block Partition (DEBP). Different selections of dominating sets may result in different edge block partitions since a linked graph may have several dominating sets. As a result, the dominating set is considered an input to the suggested framework and is chosen (or supplied) by the dealer in accordance with the application's specifications.

Let$D = \{d_1, d_2, \dots, d_k\} \subseteq V$be the chosen dominant set. Once D has been fixed, the dealer uses a deterministic assignment rule to assign each edge to exactly one dominating vertex in order to construct the edge blocks.

For each edge$e = (u, v) \in E$,determine the edge-to-dominating-vertex distance using$\delta(e, d) = min\{dist(u, d), dist(v, d)\}$,where the shortest-path distance in G is indicated by $dist(\cdot, \cdot)$.

A mapping $\phi: \mathrm{E} \rightarrow \mathrm{D}$describes the edge assignment where the dominating vertex with the smallest edge-to-dominating-vertex distance is represented by the image $\phi(e)$ for each edge $e \in E$. In other words,$\phi(e) = d_i$if$\delta(e, d_i) \leq \delta(e, d_j), \forall\, d_j \in D$.

Assigning the edge to the dominating vertex with the smallest vertex index resolves a tie when two or more dominating vertices have the same minimum edge-to-dominating-vertex distance from e. As a result, a single dominating vertex is allocated to each edge.
The dominating vertex d_i's corresponding edge blockis described as

$B_i = \phi^{-1}(d_i) = \{e \in E: \phi(e) = d_i\}$.
Thus, the group of edge blocks$\mathscr{B} = \{B_1, B_2, \dots, B_k\}$creates an edge set partition that satisfies$E = \bigcup_{i=1}^{k} B_iandB_i \cap B_j = \emptyset,\ i \neq j$.
As a result, each edge block is uniquely linked to a dominating vertex, and each edge belongs to exactly one edge block.

The resulting Dominating Edge Block Partition is uniquely determined for the pair (G,D) because the deterministic edge assignment rule and the dominating set D are both fixed prior to execution.The suggested structure is predicated on the availability of a dominating set D. When there are several minimum dominating sets, the dealer chooses one based on a specified deterministic criterion (e.g., lexicographically smallest minimum dominating set or any application-specific option). This guarantees consistency in edge block formation, share generation, and secret reconstruction since any dealer using the suggested approach on the same graph and the same dominating set will get an identical edge partition.

Theorem 4.1 (Existence of the Dominating Edge Block Partition)

Let$G = (V, E)$be a connected graph.Let$D = \{d_1, d_2, \dots, d_k\} \subseteq V$be a chosendominating set of G.Assume that the deterministic edge assignment rule outlined in Section 4 assigns each edge $e \in E$ to a dominating vertex. Then

there exists a collection of edge blocks $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ such that $E = \bigcup_{i=1}^{k} B_i$ and $B_i \cap B_j = \emptyset, i \neq j$.

Proof

The deterministic edge assignment rule calculates the edge-to-dominating-vertex distance $\delta(e, d) = \min\{\text{dist}(u, d), \text{dist}(v, d)\}$, for each edge $e = (u, v) \in E$

The edge is assigned to the dominating vertex having the minimum value of $\delta(e, d)$.

The dominant vertex with the smallest vertex index is chosen to settle a tie if two or more dominating vertices reach the same minimum distance. As a result, each edge has a single dominating vertex assigned to it.

Define $B_i = \{e \in E : \phi(e) = d_i\}$ for each dominating vertex d_i.

Every edge belongs to one of the sets B_i since each edge is assigned precisely once.
Consequently, $E = \bigcup_{i=1}^{k} B_i$.

Additionally, since an edge cannot be allocated to two distinct dominant vertices at the same time, $B_i \cap B_j = \emptyset, i \neq j$.
Thus, the set $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ creates a division of the edge set E.

As a result, every connected graph has the Dominating Edge Block Partition along with a chosen dominating set.

Theorem 4.2 (Uniqueness of DEBP for a Fixed Dominating Set)

The resulting edge partition is unique if the deterministic assignment rule, the chosen dominating set D, and the graph G are all fixed.

5. Proposed Graph Access Secret Sharing Scheme

5.1 System Model

The following elements make up the suggested graph-access secret sharing mechanism.

- Dealer ($\mathcal{D}$): The reliable authority in charge of choosing the dominating set, creating the Dominating Edge Block Partition (DEBP), producing the edge labels, calculating the block shares, and allocating the shares to the participants.
- Participants ($\mathcal{P}$): A participant is represented by each vertex in the graph. Consequently, $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.
- Dominating Participants: The dealer's primary block shares are distributed to the participants that match the chosen dominating set $D = \{d_1, d_2, \ldots, d_k\}$.
- Non-dominating Participants: Auxiliary data related to their incident edges is sent to the remaining participants. Although they help with verification or local graph information, these auxiliary variables are insufficient to independently reconstruct the secret.

5.2 Public Parameters

- Connected graph $G = (V, E)$
- Dominating set $D = \{d_1, d_2, \ldots, d_k\}$
- DEBP operator $\mathcal{D}(G, D) = \{B_1, B_2, \ldots, B_k\}$

Only the edge labels are kept confidential.

5.3 Dealer Algorithm

Input

- Secret S
- Connected graph G
- Dominating set D

Output

- Block shares $\sigma_1, \sigma_2, \ldots, \sigma_k$.

Step 1Construct the DEBP

Using the deterministic edge assignment process outlined in Section 4, create

$\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$

Step 2Generate Edge Labels

Assume $m = |E|$.

The dealer produces at random $m-1$ integers $r_1, r_2, \ldots, r_{m-1}$.
The final edge label is calculated as $r_m = S - \sum_{i=1}^{m-1} r_i$.

Therefore, $S = \sum_{i=1}^{m} r_i$.

Each edge e_i is given the corresponding label r_i.

Step 3 Calculate Block Shares

For every edge block B_i, the dealer calculates $\sigma_i = \sum_{e_j \in B_i} r_j$

Since $\{B_1, B_2, \ldots, B_k\}$ creates a division of the edge set $\sum_{i=1}^{k} \sigma_i = S$

Step 4 Distribution of Shares

Each block share is distributed by the dealer, σ_i to the individual who is associated with the dominant vertex d_i.

In other words, $d_i \leftarrow \sigma_i$, $1 \le i \le k$

An auxiliary share is given to each non-dominating vertices based on the edge labels that are incident to that vertex as

$$\tau(v) = \sum_{e \in E(v)} r_e,$$

where $E(v)$ is the set of edges incident to v.

The dealer provides information to each participant. The principal block shares used for secret reconstruction are given to participants who match the chosen dominating set, while auxiliary shares derived from the labels of their incident edges are given to the remaining participants. By themselves, these auxiliary shares do not reveal the secret or make it possible to reconstruct it, but they do maintain the participation of all graph vertices in the framework.

5.4 Secret Reconstruction

By gathering the block shares from the authorized participant set connected to the chosen dominating set, the secret is recreated.

The dealer (or a combiner with authorization) calculates $S = \sum_{i=1}^{k} \sigma_i$.

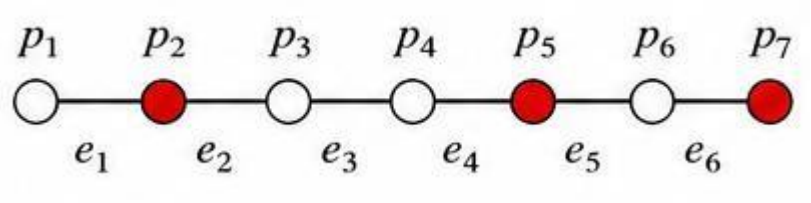
Since the edge blocks form a partition of the edge set, $\sum_{i=1}^{k} \sigma_i = \sum_{J=1}^{m} r_j = S$.

As a result, the original secret is accurately recovered.

6. Illustrative Examples

This section illustrates how the suggested DEBP framework can be applied to various graph families.

Example 6.1: Path Graph P_7



The dealer selectsdominating set $D = \{p_2, p_5, p_7\}$

Edge blocks $B_1 = \{e_1, e_2\}, B_2 = \{e_3, e_4, e_5\}, B_3 = \{e_6\}$

Dominating Edge Block Partition $\mathcal{B} = \{B_1, B_2, B_3\}$

Secret $S = 60$

Edge	e_1	e_2	e_3	e_4	e_5	e_6
Label	8	12	7	10	15	8

Block Shares: $\sigma_1 = 8 + 12 = 20$, $\sigma_2 = 7 + 10 + 15 = 32$, $\sigma_3 = 8$

Share Distribution

Dominating participant shares

Vertex(Participant)	Share
p_2	20
p_5	32
p_7	8

Auxiliary shares (for Non-Dominating participants)

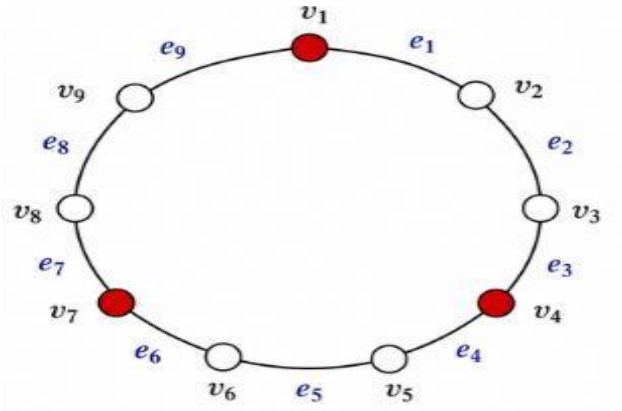
Vertex(Participant)	Incident edges	share
p_1	$\{e_1\}$	8
p_3	$\{e_2, e_3\}$	19
p_4	$\{e_3, e_4\}$	17
p_6	$\{e_5, e_6\}$	23

Secret Reconstruction

The authorized participants contribute their block shares 20, 32, 8.

$S = \sigma_1 + \sigma_2 + \sigma_3 = 60$

Example 6.2: Cycle Graph C_9



The dealer selectsdominating set $D = \{v_1, v_4, v_7\}$

Deterministic Edge Assignment

Edge $e = (u, v)$	Distance to			Assigned to$\phi(e)$
	v_1	v_4	v_7	
e_1	0	2	3	v_1
e_2	1	1	4	v_1
e_3	2	0	3	v_4
e_4	3	0	2	v_4
e_5	4	1	1	v_4
e_6	3	2	0	v_7
e_7	2	3	0	v_7
e_8	1	4	1	v_1
e_9	0	3	2	v_1

Edge blocks $B_1 = \phi^{-1}(v_1) = \{e_1, e_2, e_8, e_9\}, B_2 = \phi^{-1}(v_4) = \{e_3, e_4, e_5\}, B_3 = \phi^{-1}(v_7) = \{e_6, e_7\}$

Dominating Edge Block Partition $\mathcal{B} = \{B_1, B_2, B_3\}$

Secret $S = 90$

Edge Label Assignment

Edge	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9
Label	8	10	12	9	11	13	7	14	6

Block Shares: $\sigma_1 = 8 + 10 + 14 + 6 = 38, \sigma_2 = 12 + 9 + 11 = 32, \sigma_3 = 13 + 7 = 20$

Share Distribution

Dominating participant shares

Vertex (Participant)	Share
v_1	38
v_4	32
v_7	20

Auxiliary shares (for Non-Dominating participants)

Vertex (Participant)	Incident edges	share
v_2	$\{e_1, e_2\}$	18

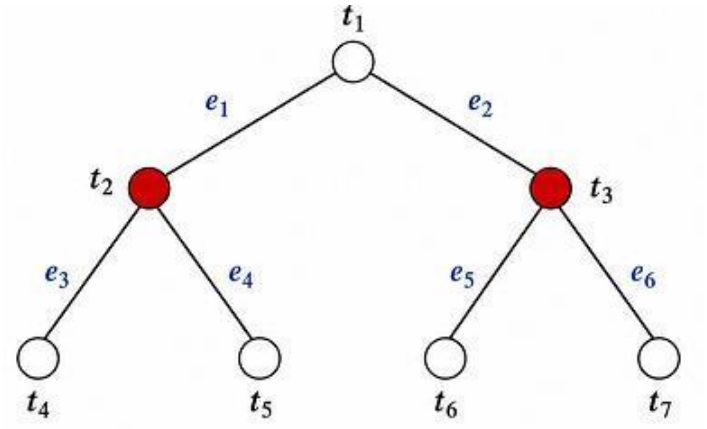
v_3	$\{e_2, e_3\}$	22
v_5	$\{e_4, e_5\}$	20
v_6	$\{e_5, e_6\}$	24
v_8	$\{e_7, e_8\}$	21
v_9	$\{e_8, e_9\}$	20

Secret Reconstruction

The authorized participants contribute their block shares 38, 32, 20.

$S = \sigma_1 + \sigma_2 + \sigma_3 = 90$

Example 6.3: Complete Binary Tree T_7



The dealer selectsdominating set $D = \{t_2, t_3\}$

Deterministic Edge Assignment

Edge $e = (u, v)$	Distance to		Assigned to $\phi(e)$
	t_2	t_3	
e_1	0	1	t_2
e_2	1	0	t_3
e_3	0	2	t_2
e_4	0	2	t_2
e_5	2	0	t_3
e_6	2	0	t_3

Edge blocks $B_1 = \phi^{-1}(t_2) = \{e_1, e_3, e_4\}, B_2 = \phi^{-1}(t_3) = \{e_2, e_5, e_6\}$

Dominating Edge Block Partition $\mathcal{B} = \{B_1, B_2\}$

Secret $S = 72$

Edge Label Assignment

Edge	e_1	e_2	e_3	e_4	e_5	e_6
Label	9	13	10	11	15	14

Block Shares; $\sigma_1 = 9 + 10 + 11 = 30$, $\sigma_2 = 13 + 15 + 14 = 42$

Share Distribution

Dominating participant shares

Vertex(Participant)	Share
t_2	30
t_3	42

Auxiliary shares (for Non-Dominating participants)

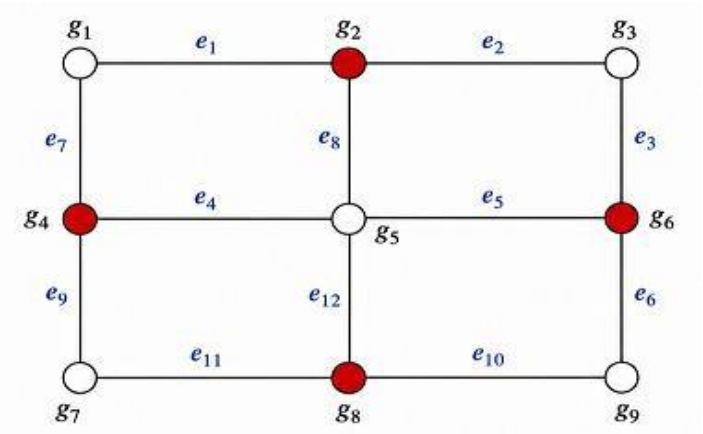
Vertex(Participant)	Incident edges	share
t_1	$\{e_1, e_2\}$	22
t_4	$\{e_3\}$	10
t_5	$\{e_4\}$	11
t_6	$\{e_5\}$	15
t_7	$\{e_6\}$	14

Secret Reconstruction

The authorized participants contribute their block shares 30,42.

Authorized combiner reconstructs the secret by computing$S = \sigma_1 + \sigma_2 = 72$.

Example 6.4: Grid Graph $P_3 \square P_3$



The dealer selectsdominating set $D = \{g_2, g_4, g_6, g_8\}$

Deterministic Edge Assignment

Edge $e = (u, v)$	Distance to				Assigned to $\phi(e)$
	g_2	g_4	g_6	g_8	
e_1	0	1	2	2	g_2
e_2	0	2	1	2	g_2
e_3	1	2	0	1	g_6
e_4	1	0	1	1	g_4
e_5	1	1	0	1	g_6
e_6	2	2	0	1	g_6
e_7	1	0	2	2	g_4
e_8	0	1	1	1	g_2
e_9	2	0	2	1	g_4

e_{10}	2	2	1	0	g_8
e_{11}	2	1	2	0	g_8
e_{12}	1	1	1	0	g_8

Edge blocks:
$B_1 = \phi^{-1}(g_2) = \{e_1, e_2, e_8\}, B_2 = \phi^{-1}(g_4) = \{e_4, e_7, e_9\}, B_3 = \phi^{-1}(g_6) = \{e_3, e_5, e_6\}, B_4 = \phi^{-1}(t_8) = \{e_{10}, e_{11}, e_{12}\}$

Dominating Edge Block Partition $\mathcal{B} = \{B_1, B_2, B_3, B_4\}$

Secret $S = 120$

Edge Label Assignment

Edge	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}
Label	7	9	10	8	12	11	6	14	13	9	10	11

Block Shares: $\sigma_1 = 7 + 9 + 14 = 30$, $\sigma_2 = 8 + 6 + 13 = 27$, $\sigma_3 = 10 + 12 + 11 = 33, \sigma_4 = 9 + 10 + 11 = 30$

Share Distribution

Dominating participant shares

Vertex(Participant)	Share
g_2	30
g_4	27
g_6	33
g_8	30

Auxiliary shares (for Non-Dominating participants)

Vertex(Participant)	Incident edges	share
g_1	$\{e_1, e_7\}$	13
g_3	$\{e_2, e_3\}$	19
g_5	$\{e_4, e_5, e_8, e_{12}\}$	45
g_7	$\{e_9, e_{11}\}$	23
g_9	$\{e_6, e_{10}\}$	20

Secret Reconstruction

The authorized participants contribute their block shares 30,27,33,30.

Authorized combiner reconstructs the secret by computing $S = \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 = 120$.

7. Computational Complexity Analysis

This section investigates the computational complexity of the proposed framework by considering each phase of the algorithm separately, namely DEBP building, edge label assignment, block share computation, share distribution, and secret reconstruction.

7.1 Dominating Set Selection

For any graph, the Minimum Dominating Set problem is NP-hard. The dominating set is presumed to have been chosen by the dealer prior to the DEBP algorithm's execution in the suggested framework. Depending on the application, an exact or heuristic algorithm may be used to obtain a dominating set when one is not available.

This step is not included in the scope of the DEBP creation because its complexity is dependent on the method used.

7.2 DEBP Construction

Each edge is assigned to a single dominating vertex by the DEBP method.To get the closest dominating vertex for each edge $e \epsilon E$, the shortest-path distance to each of the k dominating vertices is calculated. The shortest-path distances between one dominating vertex and every vertex, in the worst scenario, need$O\ (n+m)$time.This procedure must be repeated for each of the k dominating vertices. So requires $O(k(n+m))$ .Each of the m edges is evaluated and allocated to the closest dominating vertex once the distances have been calculated. This stage necessitates that each assignment compare the distances to all k dominating vertices. So this stage requires $O\ (mk)$time.

Consequently, the DEBP construction's overall complexity is $T_{DEBP} = O(k(n+m)+mk)$.

7.3 Edge Label Assignment

There is just one label assigned to each edge. Given that the graph has m edges, the edge-label assignment requires $T_{label} = O(m)$.

7.4 Block Share Computation

Because the DEBP partitions the edge set, each edge label contributes to precisely one block share. As a result, every edge is processed once, providing $T_{share} = O(m)$.

7.5 Share Distribution

Each dominating participant receives one primary block share from the dealer, while each remaining participant receives one auxiliary share. Given that each participant is given a single share, $T_{distribution} = O(n)$.

7.6 Secret Reconstruction

The authorized combiner adds up the k primary block shares during reconstruction. This results in $T_{reconstruction} = O(k)$, requiring k additions.

7.7 Total Complexity of Computation

Combining the complexity of each phase yields the overall computational complexity of the suggested framework:

$$T_{total} = T_{DEBP} + T_{label} + T_{share} + T_{distribution} + T_{reconstruction}$$
$$= O(k(n+m)+mk) + O(m) + O(m) + O(n) + O(k).$$

Given that $O(k(n+m)+mk)$ including the remaining terms, the suggested framework's total computing complexity is$T_{total} = O(k(n+m)+mk)$.

8. Conclusion

The Dominating Edge Block Partition (DEBP), a graph-theoretic operation, was presented in this paper along with an example of how to use it to build a framework for graph-access secret sharing. The suggested DEBP operator divides the edge set into pairwise disjoint connected edge blocks, each of which is uniquely linked to a dominating vertex, given a connected graph and a dominating set. Share generation, share distribution, and secret reconstruction all rely on this division.

The effectiveness of the framework has been illustrated through detailed constructions on representative graph classes, namely path graphs, cycle graphs, complete binary trees, and grid graphs. These examples demonstrate that the proposed DEBP framework is applicable to a wide variety of graph structures while maintaining a uniform construction procedure.

The proposed framework introduces a new perspective for integrating graph-theoretic operations with graph-access secret sharing and provides a mathematical foundation for further investigations into domination-based cryptographic constructions.

9. Future Work

The suggested framework provides a number of exciting avenues for further investigation.

1. To explore its structural characteristics and applicability, the DEBP operator can be expanded to weighted, directed, bipartite, planar, interval, chordal, and other specific graph classes.
2. Adaptive DEBP algorithms that effectively update edge blocks without recreating the entire partition may be developed in dynamic graph environments, where vertices or edges are added or removed over time.
3. An intriguing avenue for additional graph-theoretic research is theoretical studies of the existence, uniqueness, stability, and optimality of Dominating Edge Block Partitions for different graph families.
4. To support secure distributed applications, the suggested architecture could be expanded by adding verifiability, authentication, and integrity verification techniques.
5. Distributed storage systems, wireless sensor networks, Internet of Things (IoT) environments, block chain-based distributed systems, cloud storage architectures, and secure collaborative computing are some areas where DEBP may find use.
6. Lastly, the idea of Dominating Edge Block Partition may be used to define novel graph invariants, graph decomposition methods, and graph algorithms outside of the realm of secret sharing, creating new avenues for study in applied cryptography and graph theory.

In conclusion, a new graph-theoretic framework that links dominance, edge partitioning, and graph-access secret sharing is offered via the suggested Dominating Edge Block Partition. This framework is anticipated to promote additional study on graph operations and their applications in discrete mathematics and cryptography, as well as safe information dissemination.

Data Availability

No data were used to support the findings of the study.

Conflicts of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Financial Support

The authors have received no financial support for this work.

Reference

1. A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

2. G. R. Blakley, "Safeguarding Cryptographic Keys," in *Proc. AFIPS National Computer Conference*, vol. 48, 1979, pp. 313–317.

3. M. Ito, A. Saito, and T. Nishizeki, "Secret Sharing Scheme Realizing General Access Structure," *Electronics and Communications in Japan*, vol. 72, no. 9, pp. 56–64, 1989.

4. M. Ito, A. Saito, and T. Nishizeki, "Multiple Assignment Scheme for Sharing Secret," *Journal of Cryptology*, vol. 6, no. 1, pp. 15–20, 1993.

5. E. D. Karnin, J. W. Greene, and M. E. Hellman, "On Secret Sharing Systems," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 35–41, 1983.

6. E. F. Brickell, "Some Ideal Secret Sharing Schemes," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 9, pp. 105–113, 1989.

7. C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, "On the Information Rate of Secret Sharing Schemes," *Journal of Cryptology*, vol. 8, no. 2, pp. 83–90, 1995.

8. A. Beimel, "Secret-Sharing Schemes: A Survey," in *Coding and Cryptology*, Lecture Notes in Computer Science, vol. 6639, Berlin, Germany: Springer, 2011, pp. 11–46.

9. D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. Boca Raton, FL, USA: CRC Press, 2006.

10. D. R. Stinson, "An Explication of Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 2, no. 4, pp. 357–390, 1992.

11. J. Benaloh and J. Leichter, "Generalized Secret Sharing and Monotone Functions," in *Advances in Cryptology—CRYPTO'88*, Lecture Notes in Computer Science, vol. 403, Berlin, Germany: Springer, 1990, pp. 27–35.

12. F. Harary, *Graph Theory*. Reading, MA, USA: Addison-Wesley, 1969.

13. J. A. Bondy and U. S. R. Murty, *Graph Theory with Applications*. London, U.K.: Macmillan, 1976.

14. N. Deo, *Graph Theory with Applications to Engineering and Computer Science*. Englewood Cliffs, NJ, USA: Prentice Hall, 1974.

15. D. B. West, *Introduction to Graph Theory*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2001.

16. B. Bollobás, *Modern Graph Theory*. New York, NY, USA: Springer, 1998.

17. R. Diestel, *Graph Theory*, 5th ed. Berlin, Germany: Springer, 2017.

18. E. J. Cockayne and S. T. Hedetniemi, "Towards a Theory of Domination in Graphs," *Networks*, vol. 7, no. 3, pp. 247–261, 1977.

19. T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, *Fundamentals of Domination in Graphs*. New York, NY, USA: Marcel Dekker, 1998.

20. T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, Eds., *Domination in Graphs: Advanced Topics*. New York, NY, USA: Marcel Dekker, 1998.

21. H.-M. Sun, H. Wang, B.-H. Ku, and J. Pieprzyk, "Decomposition Construction for Secret Sharing Schemes with Graph Access Structures in Polynomial Time," *SIAM Journal on Discrete Mathematics*, vol. 24, no. 1, pp. 133–151, 2010.

22. L. Csirmaz, "Secret Sharing Schemes on Graphs," Cryptology ePrint Archive, Report 2005/059, 2005.

23. A. Beimel, O. Farràs, and N. Peter, "Secret Sharing Schemes for Dense Forbidden Graphs," in *Security and Cryptography for Networks (SCN)*, Lecture Notes in Computer Science, Berlin, Germany: Springer, 2016.

24. A. Beimel, O. Farràs, Y. Mintz, and N. Peter, "Linear Secret-Sharing Schemes for Forbidden Graph Access Structures," *IEEE Transactions on Information Theory*, vol. 68, no. 3, pp. 2083–2100, 2022.

25. A. Beimel and O. Farràs, "The Share Size of Secret-Sharing Schemes for Almost All Access Structures and Graphs," in *Theory of Cryptography Conference (TCC)*, Lecture Notes in Computer Science, vol. 12552, Springer, 2020.

26. J. Bitar, M. Farràs, et al., "Optimal Linear Secret Sharing Schemes for Graph Access Structures on Six Participants," *Theoretical Computer Science*, vol. 771, pp. 1–8, 2019.

27. A. K. Chattopadhyay, S. Saha, A. Nag, and S. Nandi, "Secret Sharing: A Comprehensive Survey, Taxonomy and Applications," *Computer Science Review*, vol. 51, Art. no. 100608, 2024.

28. A. Drissi and M. Akdim, "A Comprehensive Review of Graph Theory Applications in Secret Sharing Schemes," *Journal of Combinatorial Mathematics and Combinatorial Computing*, vol. 123, pp. 61–73, 2024.

29. D. Francati and D. Venturi, "Evolving Secret Sharing Revisited: Computational Security and Succinctness," *Designs, Codes and Cryptography*, 2025.

30. R. Cramer, V. Daza, I. Gracia, J. Jiménez Urroz, N.-G. Leander, J. Martí-Farré, and C. Padró, "On Codes, Matroids, and Secure Multiparty Computation from Linear Secret-Sharing Schemes," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2644–2657, 2008