mathematics

MDPI

Article

Optimal Shadow Allocations of Secret Sharing Schemes Arisen from the Dynamic Coloring of Extended Neighborhood Coronas

Raúl M. Falcón [1,*], Nagaraj Mohanapriya [2] and Venkitachalam Aparna [2]

[1] Department Applied Mathematics I, School of Architecture, Universidad de Sevilla, 41012 Sevilla, Spain
[2] PG and Research Department of Mathematics, Kongunadu Arts and Science College, Coimbatore 641029, Tamil Nadu, India; n.mohanamaths@gmail.com (N.M.); aparnav18794@gmail.com (V.A.)
* Correspondence: rafalgan@us.es

Abstract: Every t-dynamic proper n-coloring of a graph G describes a shadow allocation of any $(n, t+1)$-threshold secret sharing scheme based on G, so that, after just one round of communication, each participant can either reconstruct the secret, or obtain a different shadow from each one of his/her neighbors. Thus, for just one round of communication, this scheme is fair if and only if the threshold is either less than or equal to the minimum degree of G, or greater than or equal to its maximum degree. Despite that the dynamic coloring problem has widely been dealt with in the literature, a comprehensive study concerning this implementation in cryptography is still required. This paper delves into this topic by focusing on the use of extended neighborhood coronas for modeling communication networks whose average path lengths are small even after an asymptotic growth of their center and/or outer graphs. Particularly, the dynamic coloring problem is solved for any extended neighborhood corona with center path or star, for which we establish optimal shadow allocations of any (fair) threshold secret sharing scheme based on them. Some bounds are also established for the dynamic chromatic number of any extended neighborhood corona.

Keywords: dynamic coloring; extended neighborhood corona; threshold secret sharing scheme

MSC: 05C15; 94A62

check for updates

Citation: Falcón, R.M.; Mohanapriya, N.; Aparna, V. Optimal Shadow Allocations of Secret Sharing Schemes Arisen from the Dynamic Coloring of Extended Neighborhood Coronas. *Mathematics* **2022**, *10*, 2018. https://doi.org/10.3390/math10122018

Academic Editor: Angel Martín-del-Rey

Received: 1 May 2022
Accepted: 9 June 2022
Published: 11 June 2022

1. Introduction

In 1998, Watts and Strogatz [1] introduced small-world networks as graphs with small average path length and large clustering coefficient. If both conditions are preserved after a dynamical growth of their order and size, they may represent complex networks [2]. Some complex networks such as electrical or biological ones share this property, but they have small clustering coefficient [3,4].

Products of graphs efficiently model the growth of networks [5]. One may find examples in this regard concerning Cartesian product [6,7], hierarchical product [8], or Kronecker product [9,10], amongst others. Of particular interest for the aim of this paper, is the remarkable recursive use of corona products [11–15] for modeling small-world networks. This paper delves into this topic by focusing on extended neighborhood coronas with small average path length on which an (n, t)-threshold secret sharing scheme can be implemented so that, after just one round of communication, each participant can either reconstruct the secret, or obtain a different shadow from each neighbor. Introduced independently by Shamir [16] and Blakley [17], secret sharing schemes consist of two phases. During the first one, a dealer splits a secret into n pieces of information or shadows. Copies of these pieces are distributed among a group of participants. Then, there is a reconstruction phase in which any authorized subgroup sharing at least t distinct shadows suffices to reconstruct the secret, whereas no subgroup sharing less than t distinct shadows can perform it. Thus, secret sharing schemes are particularly relevant in online storage and cloud computing because they enforce data security among the nodes of the network [18].

A secret sharing scheme is said to be fair if, once the reconstruction phase is finished, a participant can recover the secret if and only if all other participants can also recover it. Even if every secret sharing scheme should ensure a fair reconstruction of the secret, it is difficult in practice. It is mainly due to the possible existence of dishonest participants who obtain information from the honest ones, but either do not share their own shadows or share fake ones. Of course, the dealer must also be honest to ensure fairness.

The first fair secret sharing scheme was described by Tompa and Woll [19], who proposed to hide the secret in a constant sequence of a dummy secret. Multiple rounds of simultaneous communications among participants are then required to reconstruct the original secret. Lin and Harn [20] also proposed to hide it, but now the sequence is formed by random dummy secrets. The one placed just after the original secret is made public at the beginning of the reconstruction phase. Again, multiple rounds of communications are required, but now, the simultaneous release of shadows is not necessary. As an alternative solution, He and Dawnson [21] proposed a slow-information-revealing process by sharing the secret bit by bit. It was the first time in which formal proofs concerning the behavior of this reconstruction process were given. Particularly, the rate of revealed information was estimated at each round of the reconstruction phase.

All the previous solutions yield a Nash equilibrium. Nevertheless, they are difficult to implement without strong communication channels or supporting procedures. Due to this, fair secret sharing schemes have also been dealt with in the literature by making use of probabilistic and game-theoretic techniques. Thus, for example, Laih and Lee [22] proposed a v-fairness (n, t)-secret sharing scheme in which, even if $v < t/2$ participants were dishonest, the remaining ones would have equal probability to obtain the secret without the requirement of a simultaneous release of their shadows. In their proposal, the secret is decomposed into three subsecrets so that any two of them give rise to the secret. Then, the reconstruction phase consists of three rounds, so that even if cheaters could obtain the secret in the first two rounds, the honest participants could also obtain it in the third one. The efficiency of this protocol was later improved by Hwang and Chang [23] and Lee [24].

Furthermore, in order to describe more accurate modelings, Halpern and Teague [25] proposed to deal not with dishonest participants, but rational ones, who will deviate from the reconstruction protocol if and only if it is in their interest to do so. Such participants prefer to obtain the secret over not obtaining it, but they also prefer that as few as possible of the other participants reconstruct the secret. Thus, in general, these rational participants have no incentive to share their shadows. It makes it very difficult to obtain fairness, unless nobody reconstructs the secret. In this context, Ong et al. [26] described a simple protocol to ensure fairness with a high probability in any secret sharing scheme with a minority of honest participants and many rational participants. Based on a synchronous release of shadows, they achieved a trembling hand perfect equilibrium just after two rounds of communications in the reconstruction phase. Alternative reconstruction protocols with multiple rounds of synchronous communication have been described by Tian et al. [27], and Zhang et al. [28]. An asynchronously rational secret sharing scheme was also described by Harn et al. [29]. Notice also here that, even if multiple rounds of communications are commonly used to describe fair secret sharing schemes, they give usually rise to large overheads. Due to this, the description of new fair secret sharing schemes with only one round of communication constitutes a current area of research [30–32].

From here on, all the communication networks under consideration are assumed to be finite, simple, and connected undirected graphs. This paper deals with secret sharing schemes based on these graphs, where each node represents a participant of the scheme, and two nodes are connected by an edge if and only if there exists some proximity relationship among them so that they can cooperate to reconstruct the secret. More specifically, one round of communication among nodes implies that each participant receives the shadows of her/his adjacent participants. In 1991, Naor and Roth [33] already considered this type of scheme as a way to split an arbitrary computer file into pieces of information and distribute them among a network of processors so that each node constitutes a memory device. In order to reconstruct the content of the original file, each device can access its own memory and those ones of its adjacent nodes. The objective is minimizing the total amount of data stored and ensuring an efficient reconstruction of the original file, even in the case of network failures or attacks [34,35]. A comprehensive study of the network topology is, therefore, necessary to design an optimal storage allocation of data among the nodes [36]. To this end, it can be assumed, without loss of generalization, that no two neighbors have the same information data. Under these assumptions, any shadow allocation among the nodes of a graph on which an (n, t)-threshold secret sharing scheme is based constitutes an n-proper multicoloring of the corresponding graph. Here, each color represents a shadow of the secret. Thus, for example, Naor and Roth [33] already defined a multicoloring to minimize the total size of memory in a network of processors. Notice that a multicoloring becomes an n-proper coloring whenever each participant has exactly one shadow. In this paper, we assume this last condition by making use of Montgomery's dynamic coloring [37,38] in order to describe the corresponding shadow allocation. Let us detail this fact in the following paragraph.

In 2017, Kim and Ok [39] realized that every t-dynamic proper n-coloring of a graph G describes a shadow allocation of any $(n, t+1)$-threshold secret sharing scheme based on G. This scheme satisfies that, after just one round of communication among nodes, each participant can either reconstruct the secret or obtain a different shadow from each one of his/her neighbors. More specifically, any such coloring c is defined so that the number of colors or shadows in the neighborhood $N_G(v)$ of every vertex v holds that

$$|c(N_G(v))| \geq \min\{t, |N_G(v)|\}. \tag{1}$$

If all the participants were honest, then this scheme is fair if and only if either $t \leq \delta(G)$ or $t \geq \Delta(G)$. Here, $\delta(G)$ and $\Delta(G)$ denote, respectively, the minimum and maximum degrees of the graph. If $t \leq \delta(G)$, then all the participants would reconstruct the secret in one round of communication, while none of them could reconstruct it if $t \geq \Delta(G)$. The following pair of main problems arise here.

Problem 1. *Which is the minimum number of rounds of communication that are necessary to ensure that the secret can be reconstructed by all the participants?*

Problem 2. *Which is the minimum number of distinct shadows in which the secret has to split to ensure condition (1)?*

Both problems depend clearly on the parameter t and the underlying network topology. Thus, for instance, the solution of Problem 1 is 1, if $t \leq \delta(G)$, while it is upper-bounded by the diameter of the graph otherwise. Furthermore, the minimum value referred to in Problem 2 constitutes, indeed, the t-dynamic chromatic number $\chi_t(G)$. In this way, every t-dynamic proper $\chi_t(G)$-coloring of a graph G constitutes an optimal shadow allocation among the nodes. Computing the t-dynamic chromatic number of a graph constitutes the t-dynamic coloring problem for G. If $t = 1$, then it coincides with the classical coloring problem. Despite that the case $t \geq 2$ has widely been dealt with in the literature, there exists only some partial results concerning corona products [40] and generalized corona products [41,42]. Particularly, Aparna and Mohanapriya [43] have recently dealt with the dynamic problem for extended neighborhood coronas whose center is a complete graph.

To the best knowledge of the authors, there is no comprehensive study in the literature concerning Kim and Ok's secret sharing schemes. This paper delves into this topic by solving Problems 1 and 2 for any extended neighborhood corona whose center is either a path or a star. To this end, we assume the honesty of all the participants. A much deeper analysis is required for those cases in which one also assumes the existence of dishonest and/or rational participants. It is established as further work. The choice of extended neighborhood coronas with a center path or star is due to two main reasons, which are comprehensively analyzed throughout the paper. First, they enable one to model complex networks whose average path lengths remain small even after an asymptotic growth of their centers and/or outer graphs. The second one is related to Problem 1, because both types of graphs enable the reconstruction of the secret by all the participants in, at most, two rounds of communications, whenever, of course, everybody is honest.

The paper is organized as follows. In Section 2, we describe some preliminary concepts and results on graph theory that are used throughout the manuscript. Then, Section 3 deals with those parameters describing any extended neighborhood corona. Particularly, their average path length and clustering coefficient are established in Lemma 3. Then, Proposition 1 shows that the asymptotic behavior of the former is equivalent to that one of the average path length of the center graph under consideration. Depending on whether the latter is unbounded or not, the dynamical growth of these graphs differs to keep their average path length small. In order to illustrate both cases, we focus our study on extended neighborhood coronas whose centers are either a path or a star. Theorems 1 and 2 in Section 4 solve their respective dynamic coloring problems. Some bounds are also established for the dynamic chromatic number of any extended neighborhood corona.

2. Preliminaries

This section deals with some preliminary concepts, notations, and results on graph theory that are used throughout the paper. For more details about this topic, we refer the reader to the classical manuscript of Harary [44].

A graph G is a pair formed by a set $V(G)$ of vertices and a set $E(G)$ of edges, so that every edge $vw \in E(G)$ contains two adjacent vertices $v, w \in V(G)$. If $v = w$, then the edge is a loop. A graph is simple if it contains no loops and no two edges join the same pair of vertices. Further, the cardinalities of $V(G)$ and $E(G)$ are, respectively, the order and the size of the graph. A graph is finite if both its order and its size are finite. All the graphs in this paper are simple and finite.

The complete graph K_n is a graph of order n, whose vertices are pairwise adjacent. It is a triangle if $n = 3$. A clique of a graph G is any set of vertices of a complete graph within G. The clique number $\omega(G)$ is the largest order of any clique of G. The neighborhood $N_G(v)$ of a vertex $v \in V(G)$ is the set of vertices that are adjacent to v. Its degree $\deg_G(v)$ is the cardinality of this set. A vertex is pendant if it has degree of one. The minimum and maximum vertex degrees of the graph G are, respectively, denoted by $\delta(G)$ and $\Delta(G)$. Further, a path P_n, with $n > 2$, is any ordered sequence of adjacent and pairwise distinct vertices $\langle v_1, \ldots, v_n \rangle$. The star S_n, with $n > 2$, is a graph formed by n pendant vertices and a center vertex of degree n.

In 1970, Frucht and Harary [45] introduced the corona product $G \odot H$ of center G, with $V(G) = \{v_1, \ldots, v_n\}$, and outer graph H as the graph resulting from G and n copies of H, so that each vertex v_i is joined to every vertex in the ith copy of H. Much more recently, Indulal [46] introduced the neighborhood corona $G \star H$ as the graph resulting from G and n copies of H, so that every vertex in $N_G(v_i)$ is joined to every vertex in the ith copy of H. Five years later, Adiga et al. [47] defined the extended neighborhood corona $G * H$ as the graph resulting from $G \star H$ after connecting every vertex in the ith copy of H to every vertex of the jth copy of H, whenever $v_iv_j \in E(G)$. Figure 1 illustrates these three products.

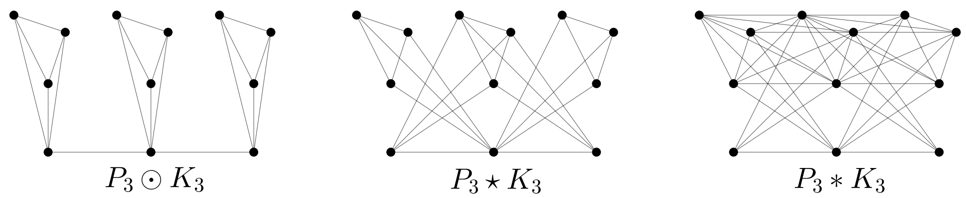

Figure 1. Corona, neighborhood corona, and extended neighborhood corona of P_3 and K_3.

The distance $d_G(v,w)$ between two vertices $v,w \in V(G)$ is the size of any shortest path in G connecting both vertices. The diameter $\mathrm{diam}(G)$ of the graph is the maximum distance between any pair of its vertices. The average path length of the graph G is

$$\ell_G := \frac{1}{|V(G)| \cdot (|V(G)|-1)} \cdot \sum_{\substack{v,w \in V(G) \\ v \neq w}} d_G(v,w).$$

An open triplet in G consists of any three vertices describing a path, but not a triangle. The clustering coefficient of the graph G is

$$\mathcal{C}_G := \frac{3 \cdot T_G}{3 \cdot T_G + \tau_G},$$

where T_G and τ_G denote, respectively, the number of triangles and open triplets in G.

A proper k-coloring of the graph G is any map assigning k distinct colors to the set $V(G)$ so that no two adjacent vertices share color. Throughout this paper, we consider the set of colors $\{0,\ldots,k-1\}$. The minimum positive integer k for which this coloring exists is the chromatic number $\chi(G)$. Any such coloring is said to be optimal. The following lemmas refer to the dynamic coloring, which has been defined in the introductory section.

Lemma 1 ([37]). *Let G be a simple finite graph and let t be a positive integer. Then,* $\min\{t,\Delta(G)\}+1 \leq \chi_t(G) \leq \chi_{t+1}(G)$. *Moreover,* $\chi_t(G) \leq \chi_{\Delta(G)}(G)$.

Lemma 2 ([48]). *Let n and t be two positive integers. Then,*

(a) *If $n>2$, then* $\chi_t(P_n) = \begin{cases} 2, & \text{if } t=1, \\ 3, & \text{otherwise.} \end{cases}$

(b) *If $n>2$, then* $\chi_t(S_n) = \min\{n,t\}+1$.

3. Extended Neighborhood Coronas

From now on, we consider an extended neighborhood corona $G * H$ of center G and outer graph H, where $V(G) = \{u_1,\ldots,u_m\}$ and $V(H) = \{v_1,\ldots,v_n\}$. For each pair of positive integers $i \leq m$ and $j \leq n$, let $H^{(i)}$ denote the ith copy of the graph H, and let $v_{i,j}$ denote the copy of the vertex $v_j \in V(H)$ in $H^{(i)}$. In what follows, we describe some basic parameters concerning the graph $G * H$. First, the degree of each vertex $v \in V(G*H)$ is

$$\deg_{G*H}(v) = \begin{cases} (n+1)\cdot \deg_G(v), & \text{if } v \in V(G), \\ (n+1)\cdot \deg_G(u_i) + \deg_H(v_j), & \text{if } v = v_{i,j}. \end{cases} \tag{2}$$

The distance between two distinct and non-adjacent vertices $v,w \in \left(\{u_i\} \cup V(H^{(i)})\right) \times \left(\{u_j\} \cup V(H^{(j)})\right)$ is

$$d_{G*H}(v,w) = \begin{cases} 2, & \text{if } i=j, \\ d_G(u_i,u_j), & \text{otherwise.} \end{cases} \tag{3}$$

As a consequence, the next lemma holds.

Lemma 3. *The extended neighborhood corona $G*H$ satisfies the following assertions.*

1. *Its order is $mn+m$.*
2. *Its size is $(n+1)^2 \cdot |E(G)| + m \cdot |E(H)|$.*
3. $\delta(G*H) = (n+1)\cdot\delta(G)$.
4. $\Delta(G*H) = (n+1)\cdot\Delta(G) + \Delta(H)$.
5. $\mathrm{diam}(G*H) = \mathrm{diam}(G)$.

6. $T_{G*H} = T_G + m \cdot T_H + 2 \cdot (n+1) \cdot |E(G)| \cdot |E(H)|$.
7. *Its number of open triplets is*

$$\begin{aligned}\tau_{G*H} =& \tau_G + m \cdot \tau_H + (n^2+n) \cdot \sum_{v \in V(G)} \deg_G(v)^2 + \\ &+ (n^3+n^2+n) \cdot \sum_{v \in V(G)} \binom{\deg_G(v)}{2} + 2mn \cdot |E(G)| \cdot \left(\binom{n}{2} + |E(H)|\right).\end{aligned}$$

8. *Its average path length is*

$$\ell_{G*H} = \frac{2 \cdot (n^2 - |E(H)|) + \ell_G \cdot (m-1)(n+1)^2}{(n+1)(mn+m-1)}.$$

Proof. The order and size follow readily from the definition of the graph. Its minimum and maximum degrees hold from (2), while its diameter follows from (3). Concerning the parameter T_{G*H}, notice that every triangle in $G*H$ contains either three vertices in G or two adjacent vertices in $H^{(i)}$, for some $i \leq m$. In this last case, the third vertex can be either in $H^{(i)}$, or in an adjacent copy, or in the graph G. Thus, the value of T_{G*H} derives from the existence of

- T_H distinct triangles of the first type;
- $n \cdot |E(H)| \cdot \deg_G(u_i)$ distinct triangles of the second type;
- $|E(H)| \cdot \deg_G(u_i)$ distinct triangles of the third type.

Notice here that $\sum_{v \in V(G)} \deg_G(v) = 2 \cdot |E(G)|$. Further, the parameter τ_{G*H} derives from the existence of

- τ_G open triplets in G;
- $n \cdot \sum_{v \in V(G)} \deg_G(v)^2$ open triplets containing an edge in G and a third vertex in a copy of H;
- $n \cdot \sum_{v \in V(G)} \binom{\deg_G(v)}{2}$ open triplets containing two non-adjacent vertices in G and the third one in a copy of H;
- $n^2 \cdot \sum_{v \in V(G)} \deg_G(v)^2$ open triplets containing two vertices in adjacent copies of H and the third one in G;
- $n^2 \cdot \sum_{v \in V(G)} \binom{\deg_G(v)}{2}$ open triplets containing one vertex in G and two vertices in non-adjacent copies of H;
- $m \cdot \tau_H$ open triplets within a same copy of H;
- $2mn \cdot |E(G)| \cdot \left(\binom{n}{2} - |E(H)|\right)$ open triplets containing two non-adjacent vertices in a same copy of H and the third one in an adjacent copy;
- $4mn \cdot |E(G)| \cdot |E(H)|$ open triplets containing an edge in a copy of H and the third one in an adjacent copy;
- $n^3 \cdot \sum_{v \in V(G)} \binom{\deg_G(v)}{2}$ open triplets containing three vertices in three adjacent copies of H.

Finally, the average path length follows from the $2 \cdot |E(H)|$ ordered pairs of adjacent vertices in each $E(H^{(i)})$, the n pairs of vertices in each $\{u_i\} \times V(H^{(i)})$, and the $2 \cdot \left(\binom{n}{2} - |E(H)|\right)$ ordered pairs of non-adjacent vertices in each $V(H^{(i)}) \times V(H^{(i)})$, all of them at distance two in $G*H$; and the fact that the sum of distances for the remaining ordered pairs of vertices in $G*H$ is $\ell_G \cdot m(m-1)(n+1)^2$. □

Based on the sixth statement of Lemma 3, the following result describes how the asymptotic behavior of ℓ_{G*H} is equivalent to that one of ℓ_G.

Proposition 1. *It is verified that*

1. $\lim_{m \to \infty} \ell_{G*H} = \frac{n+1}{n} \cdot \lim_{m \to \infty} \ell_G$.
2. $\frac{\ell_G \cdot (m-1)+1}{m} \leq \lim_{n \to \infty} \ell_{G*H} \leq \frac{\ell_G \cdot (m-1)+2}{m}$.
3. $\lim_{m,n \to \infty} \ell_{G*H} = \lim_{m \to \infty} \ell_G$.

Proof. The result holds readily from Lemma 3. In particular, the lower and upper bounds in the second statement arise from considering, respectively, $H = K_n$ and $|E(H)| = 0$. □

Let us remember our interest in modeling (fair) secret sharing schemes over any extended neighborhood corona $G * H$, whose average path length is small even after a dynamical growth of the graph, and so that every participant obtains the maximum number of shadows from his/her neighbors to obtain the secret. To this end, we may ensure from Proposition 1 that, if the asymptotic behavior of ℓ_G is unbounded, then only a growth of the outer graph is feasible. But, if ℓ_G has a bounded asymptotic behavior, then an independent growth of both the center and the outer graphs is feasible. In this paper, we illustrate both cases by focusing on the study of extended neighborhood coronas with either a center path graph P_m or a center star graph S_m. Notice here that

$$\ell_{P_m} = \frac{m+1}{3} \qquad \text{and} \qquad \ell_{S_m} = \frac{2m}{m+1}.$$

Then, for every graph H, Proposition 1 implies that

$$\frac{m^2+2}{3m} \leq \lim_{n\to\infty} \ell_{P_m*H} \leq \frac{m^2+5}{3m}, \qquad \lim_{m\to\infty} \ell_{S_m*H} = \frac{2n+2}{n},$$

$$\frac{2m^2+m+1}{(m+1)^2} \leq \lim_{n\to\infty} \ell_{S_m*H} \leq \frac{2m^2+2m+2}{(m+1)^2} \qquad \text{and} \qquad \lim_{m,n\to\infty} \ell_{S_m*H} = 2.$$

Furthermore, concerning the asymptotic behavior of the clustering coefficient $\mathcal{C}_{G*H}$, with $G \in \{P_m,\, S_m\}$ and $m > 2$, Lemma 3 implies that

$$T_{P_m*H} = m \cdot T_H + 2 \cdot (m-1)(n+1) \cdot |E(H)|,$$
$$T_{S_m*H} = (m+1) \cdot T_H + 2 \cdot m \cdot (n+1) \cdot |E(H)|,$$

$$\begin{aligned}\tau_{P_m*H} =& m - 2 + m \cdot \tau_H + (4m-6)(n^2+n) + (m-2)(n^3+n^2+n) + \\ &+ 2(m^2-m)n \cdot \left(\binom{n}{2} + |E(H)|\right)\end{aligned}$$

and

$$\begin{aligned}\tau_{S_m*H} =& (m+1) \cdot \tau_H + (m^2+m) \cdot (n^2+n) + \binom{m}{2} \cdot (n^3+n^2+n) + \\ &+ 2m^2 n \cdot \left(\binom{n}{2} + |E(H)|\right).\end{aligned}$$

Hence, $\lim_{m\to\infty} \mathcal{C}_{S_m*H} = 0$. Moreover, $\lim_{n\to\infty} \mathcal{C}_{G*H} = 0$, for any $G \in \{P_m,\, S_m\}$ such that $T_{G*H} \not\sim O(n^3)$. It is not the case if $T_{G*H} \sim O(n^3)$. Thus, for instance,

$$\lim_{n\to\infty} \mathcal{C}_{P_m*K_n} = \frac{4m-3}{6m^2+4m-9} \qquad \text{and} \qquad \lim_{n\to\infty} \mathcal{C}_{S_m*K_n} = \frac{8m+2}{15m^2-11m+8}.$$

Extended neighborhood coronas with a center path or star may, therefore, be used to model small-world networks and complex networks with small average path length. As it has been indicated in the introductory section, solving the dynamic coloring problem for these networks enables one to describe fair secret sharing schemes based on them. In the next section, we solve this problem for any graph $G * H$, with $G \in \{P_m,\, S_m\}$, and establish the asymptotic behavior of the minimum number of distinct shadows that are required for these secret sharing schemes.

4. Solving the Dynamic Coloring Problem

Let us start this section by formulating a series of preliminary results that are useful to solve the dynamic coloring problem for any extended neighborhood corona $G * H$, with $G \in \{P_m, S_m\}$. First, based on the fact that both the path P_m and the star S_m have pendant vertices, it is interesting to establish a lower bound for the dynamic chromatic number of any extended neighborhood corona $G * H$, whose center has a non-empty set of pendant vertices. We denote this set by $\mathcal{P}(G)$.

Lemma 4. *If $\mathcal{P}(G) \neq \emptyset$, then, for every positive integer t, it is*

$$\max_{u \in \mathcal{P}(G)} \left\{ \min\{t, n+1\} + \min_{v \in N_G(u)} \{t, \deg_{G*H}(v)\} \right\} \leq \chi_t(G * H).$$

Proof. Let c be an optimal t-dynamic proper coloring of the graph $G * H$, and let $u \in \mathcal{P}(G)$. The result holds readily from Condition (1). It implies that $|c(N_{G*H}(u))| \geq \min\{t, n+1\}$. Moreover, together with the underlying adjacency of the graph $G * H$, it also implies that $\min\{t, \deg_{G*H}(v)\}$ extra colors are required for every vertex $v \in N_G(u)$. □

In a more general way, we establish a pair of lower and upper bounds for the t-dynamic chromatic number of any extended neighborhood corona $G * H$.

Lemma 5. *For every positive integer t, let $\alpha_t = \min\{\lceil \frac{t}{n+1} \rceil, \Delta(G)\}$ and $\beta_t = \min\{n + 1, \max\{t, \chi(H)\}\}$. Then,*

$$\omega(G) \cdot \chi(H) \leq \chi_t(G * H) \leq \beta_t \cdot \chi_{\alpha_t}(G).$$

Proof. The lower bound follows readily from the complete adjacency among the adjacent copies $H^{(i_1)}, \ldots, H^{(i_{\omega(G)})}$, where $\{u_{i_1}, \ldots, u_{i_{\omega(G)}}\} \subseteq V(G)$ is a maximum clique within G. Concerning the upper bound, it is enough to define an appropriate t-dynamic proper coloring c of $G * H$. From Lemma 1, we may assume that $t \leq \Delta(G * H)$, and hence Lemma 3 implies that $\lceil \frac{t}{n+1} \rceil \leq \Delta(G) + 1$.

First, we define $c(u_i) = \beta_t \cdot c_G(u_i)$, for all $i \leq m$, where the map c_G is an optimal α_t-dynamic proper coloring of G. In addition, let c_H be an optimal proper coloring of the graph H. Then, for every pair of positive integers $i \leq m$ and $j \leq n$, we define

$$c(v_{i,j}) = \begin{cases} c(u_i) + c_H(v_j), & \text{if } \beta_t = \chi(H), \\ c(u_i) + j + 1, & \text{if } \beta_t = n + 1. \end{cases}$$

Finally, if $\chi(H) < t \leq n$, then it is always possible to find $t - \chi(H)$ distinct vertices in H that are not uniquely identified by the map c_H. That is, their respective colors are assigned more than once to $V(H)$. Without loss of generality, we may assume that these vertices are $v_1, \ldots, v_{t-\chi(H)}$. Then, for each $i \leq m$ and $j \leq n$, we define

$$c(v_{i,j}) = \begin{cases} c(u_i) + j - 1, & \text{if } j \leq t - \chi(H), \\ c(u_i) + t - \chi(H) + c_H(v_j), & \text{otherwise.} \end{cases}$$

In all the cases, the map c is a t-dynamic proper coloring of $G * H$. □

The following result holds readily from Lemma 5.

Proposition 2. *If $\omega(G) = \chi(G)$, then $\chi_t(G * H) = \chi(G) \cdot \chi(H)$, for every $t \leq \chi(H)$.*

4.1. Extended Neighborhood Coronas with Center Path Graphs

Based on the previous results, we may solve the dynamic coloring problem for any extended neighborhood corona $P_m * H$, where $P_m = \langle u_1, \ldots, u_m \rangle$. Here, $m > 2$.

Theorem 1. *For every positive integer t,*

$$\chi_t(P_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{if } n+1 < t < 2n+2, \\ 3n+3, & \text{otherwise.} \end{cases}$$

Proof. The case $t \leq \chi(H)$ follows readily from Proposition 2 and the fact that $\omega(P_m) = \chi(P_m) = 2$. In addition, if $t > \chi(H)$, then we have from Lemma 4 that

$$\min\{t, n+1\} + \min\{t, 2n+2\} \leq \chi_t(P_m * H). \tag{4}$$

Together with Lemma 2 and the upper bound described in Lemma 5, it implies both cases $\chi(H) < t \leq n+1$ and $t \geq 2n+2$. In order to prove that the lower bound (4) is also tight for $n+1 < t < 2n+2$, let c be an optimal t-dynamic proper 3-coloring of P_m. Then, it is enough to consider the t-dynamic proper $(n+t+1)$-coloring c' of $P_m * H$ that is described so that, for each pair of positive integers $i \leq m$ and $j \leq n$, we have that $c'(u_i) = (n+1) \cdot c(u_i)$ and

$$c'(v_{i,j}) = \begin{cases} c'(u_i) + j, & \text{if } \begin{cases} i \in \{1,2\}, \text{ or} \\ j \leq \min\{t-n-2, n\}, \end{cases} \\ c'(v_{i-2,j}), & \text{otherwise.} \end{cases}$$

□

It is not difficult to check that each one of the dynamic colorings referred to in the previous proof holds that, for every vertex $v \in V(P_m * H)$ and every color $i \in \{0, \ldots, \chi_t(P_m * H) - 1\}$, there exists at least one vertex $w \in V(P_m * H)$ that is colored by the color i and satisfies that $d_{P_m * H}(v, w) \leq 2$. As a consequence, every $(n, t+1)$-threshold secret sharing scheme that is based on the graph $P_m * H$, and associated with any of these optimal shadow allocations, satisfies that two rounds of communication are enough to ensure that all the participants can reconstruct the secret, whenever everybody is honest. As a representative example, Figure 2 illustrates the map c' described in the proof of Theorem 1 for a 6-dynamic proper coloring of the extended neighborhood corona $P_4 * P_3$. It shows an optimal shadow allocation to obtain a $(10, 7)$-threshold secret sharing scheme so that, after just one round of communication, each participant can either reconstruct the secret or obtain a different shadow from each one of his/her neighbors. Each color or shadow is indicated between parentheses as a superscript above the corresponding vertex label.

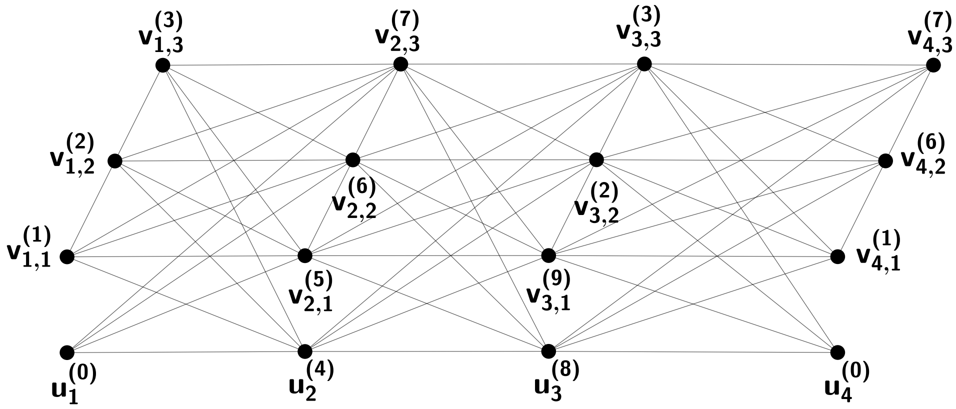

Figure 2. Optimal 6-dynamic proper coloring of $P_4 * P_3$.

From Proposition 1, the unbounded asymptotic behavior of ℓ_{P_m} implies that a small average path length of $P_m * H$ is only preserved by a dynamical growth of its outer graph. If H is large enough, then Theorem 1 implies that the minimum number of distinct shadows in which any secret must split to obtain a fair sharing scheme on $P_m * H$ is

$$\lim_{n\to\infty} \chi_t(P_m * H) = 2 \cdot \max\{t, \chi(H)\}.$$

4.2. Extended Neighborhood Coronas with Center Star Graphs

Let us finish our study by solving the dynamic coloring problem for any extended neighborhood corona $S_m * H$, where the star graph S_m has center u_1 and pendant vertices $u_2, \ldots, u_{m+1}$.

Theorem 2. *Let $m > 2$ and t be two positive integers. If H is a graph of order n, then*

$$\chi_t(S_m * H) = \begin{cases} 2 \cdot \max\{t, \chi(H)\}, & \text{if } t \le n+1, \\ n+t+1, & \text{if } n+1 < t < mn+m, \\ (m+1)\cdot(n+1), & \text{otherwise.} \end{cases}$$

Proof. The case $t \le n+1$ follows similarly to the proof of Theorem 1. In addition, if $t > n+1$, then Lemma 4 implies that

$$n + 1 + \min\{t, mn+m\} \le \chi_t(S_m * H). \tag{5}$$

Hence, the case $t \ge mn+m$ holds readily from Lemma 2 and the upper bound in Lemma 5.

In order to prove that the lower bound (5) is also tight for $n+1 < t < mn+m$, it is enough to consider the t-dynamic proper coloring c of $S_m * H$ that is described so that, for each pair of positive integers $i \le m$ and $j \le n$,

$$c(u_i) = \begin{cases} (i-1)\cdot(n+1), & \text{if } i \le 1 + \lceil \frac{t}{n+1} \rceil, \\ c(u_{i-1}), & \text{otherwise.} \end{cases}$$

and

$$c(v_{i,j}) = \begin{cases} c(u_i) + j, & \text{if } \begin{cases} i \le 1 + \lfloor \frac{t}{n+1} \rfloor, \text{ or} \\ i = 1 + \lceil \frac{t}{n+1} \rceil \text{ and } j < t \bmod (n+1), \end{cases} \\ c(v_{i-1,j}), & \text{otherwise.} \end{cases}$$

□

Similarly to the case of extended neighborhood coronas of center paths, it is not difficult to prove that two rounds of communications are enough to ensure that all the participants of a $(n, t+1)$-threshold secret sharing scheme based on $S_m * H$, and associated with any of the optimal shadow allocations referred to in the previous proof, can reconstruct the secret whenever everybody is honest. As a representative example, Figure 3 illustrates the map c described in the proof of Theorem 2 for a 7-dynamic proper coloring of the extended neighborhood corona $S_3 * P_3$. It shows the distribution of shadows to obtain an $(11, 8)$-threshold secret sharing scheme in which, after just one round of communication, each participant can either reconstruct the secret, or obtain a different shadow from each one of his/her neighbors. Again, each color or shadow is indicated between parentheses as a superscript above the corresponding vertex label.

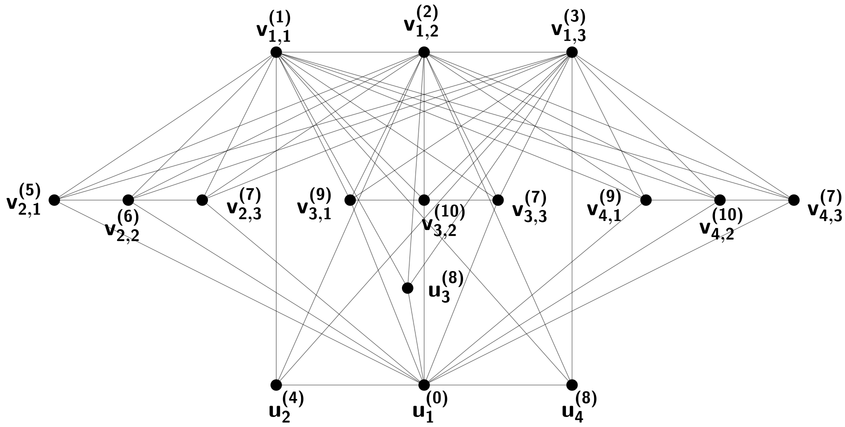

Figure 3. Optimal 7-dynamic proper coloring of $S_3 * P_3$.

From Proposition 1, the bounded asymptotic behavior of ℓ_{S_m} implies that a small average path length of $S_m * H$ is preserved by an independent dynamical growth of both its center and outer graphs. If S_m is large enough, then Theorem 1 implies that the minimum number of distinct shadows in which any secret has to split to obtain a sharing scheme on $S_m * H$ is

$$\lim_{m\to\infty} \chi_t(S_m * H) = \begin{cases} 2\cdot\max\{t,\,\chi(H)\}, & \text{if } t \leq n+1, \\ n+t+1, & \text{otherwise.} \end{cases}$$

However, if either the outer graph or both the center and the outer graphs are large enough, this minimum number of shadows is

$$\lim_{n\to\infty} \chi_t(S_m * H) = \lim_{m,n\to\infty} \chi_t(S_m * H) = 2\cdot\max\{t, \chi(H)\}.$$

5. Conclusions and Further Works

In this paper, we have studied those conditions under which an extended neighborhood corona may model a small-world network or a complex network, whose average path length is small even after some dynamical growth of the graph. Depending on the asymptotic behavior of the average path length of the center, this growth may be considered either in the outer graph, or, independently, in both the center and the outer graph. In order to illustrate both cases, our study has focused on those extended neighborhood coronas whose center is either a path or a star graph.

The dynamic coloring problem has been solved for any of these graphs. It enables one to establish the minimum number of distinct shadows in which the secret has to split to ensure that, after just one round of communication among nodes, each participant can either reconstruct the secret, or obtain a different shadow from each one of his/her neighbors. Particularly, we have proved that this value is always bounded, whatever the size of the graph is. In addition, we have proved that, whenever everybody is honest, two rounds of communications are enough to ensure that all the participants can reconstruct the secret. A much deeper analysis is required for those cases in which one also assumes the existence of dishonest and/or rational participants. It is established as further work.

In a similar, but more general, way, the following problem arises naturally for any given graph on which a threshold secret sharing scheme is based. In a first stage, it may be dealt with by assuming the honesty of all the involved participants. In a second stage, the possible existence of dishonest and/or rational participants can be assumed.

Problem 3. *Which is the minimum number of distinct shadows into which the secret has to split for ensuring that the secret can be reconstructed by everybody in, at most, k rounds of communication?*

In order to deal with this problem, it is necessary to study the shadow allocation within the k-neighborhood of each vertex v of the graph G under consideration. That is, $N_G^k(v) := \{w \in V(G) \colon d_G(v,w) \leq k\}$, where k is a positive integer. As such, a natural generalization of the concept of dynamic coloring arises. More specifically, we say that a proper n-coloring c of a graph G is a (t,k)-dynamic proper n-coloring if

$$|c(N_G^k(v))| \geq \min\{t, |N_G^k(v)|\}.$$

In this way, Problem 3 would refer to what we can call the (t,k)-dynamic chromatic number $\chi_{t,k}(G)$. If $k = 1$, then these concepts coincide with the t-dynamic proper n-coloring and the t-dynamic chromatic number described in the introductory section. A comprehensive study of these new notions is, therefore, required. It is also established as further work.

Finally, we have described in this paper some general bounds for the dynamic chromatic number of any extended neighborhood corona. Nevertheless, a more comprehensive study is required to completely solve the dynamic coloring problem for any of these graphs. It is established as further work. The results described in this paper constitute a useful starting point not only to this end, but also to delve into the description of new, fair sharing secret schemes based on other products of graphs.

Author Contributions: Conceptualization, N.M. and V.A.; methodology, R.M.F.; validation, R.M.F. and N.M.; formal analysis, R.M.F.; investigation, R.M.F., N.M. and V.A.; resources, V.A.; data curation, N.M.; writing—original draft preparation, N.M. and V.A.; writing—review and editing, R.M.F.; visualization, R.M.F.; supervision, N.M.; project administration, R.M.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Falcón's work is partially supported by the Research Project FQM-016 from Junta de Andalucía.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Watts, D.J.; Strogatz, S.H. Collective dynamics of 'small-world' networks. *Nature* **1998**, *393*, 440–442. [CrossRef]
2. Watts, D.J. *Small Worlds: The Dynamics of Networks between Order and Randomness*; Princeton University Press: Princeton, NJ, USA, 1999.
3. Ferrer i Cancho, R.; Janssen, C.; Solé, R.V. Topology of technology graphs: Small world patterns in electronic circuits. *Phys. Rev. E* **2001**, *64*, 046119. [CrossRef]
4. Newman, M.E.J. The structure and function of complex networks. *SIAM Rev.* **2003**, *45*, 167–256. [CrossRef]
5. Parsonage, E.; Nguyen, H.X.; Bowden, R.; Knight, S.; Falkner, N.; Roughan, M. Generalized graph products for network design and analysis. In Proceedings of the 19th annual IEEE International Conference on Network Protocols, Vancouver, BC, Canada, 17–20 October 2011; pp. 79–88.
6. Duchon, P.; Hanusse, N.; Lebhar, E.; Schabanel, N. Could any graph be turned into a small-world? *Theoret. Comput. Sci.* **2006**, *355*, 96–103. [CrossRef]
7. Flammini, M.; Moscardelli, L.; Navarra, A.; Pérennes, S. Asymptotically optimal solutions for small world graphs. *Theory Comput. Syst.* **2008**, *42*, 632–650. [CrossRef]
8. Qi, Y.; Yi, Y.; Zhang, Z. Topological and spectral properties of small-world hierarchical graphs. *Comput. J.* **2019**, *62*, 769–784. [CrossRef]
9. Leskovec, J.; Chakrabarti, D.; Kleinberg, J.; Faloutsos, C.; Ghahramani, Z. Kronecker graphs: An approach to modeling networks. *J. Mach. Learn. Res.* **2010**, *11*, 985–1042.
10. Moreno, S.; Neville, J.; Kirshner, S. Tied Kronecker product graph models to capture variance in network populations. *ACM Trans. Knowl. Discov. Data* **2018**, *12*, 1–40. [CrossRef]
11. Lv, Q.; Yi, Y.; Zhang, Z. Corona graphs as a model of small-world networks. *J. Stat. Mech.* **2015**, *2015*, 11024. [CrossRef]

12. Qi, Y.; Li, H.; Zhang, Z. Extended corona product as an exactly tractable model for weighted heterogeneous networks. *Comput. J.* **2018**, *61*, 745–760. [CrossRef]
13. Rajkumar, R.; Muthuraman, S. Structural and spectral properties of the generalized corona networks. *Int. J. Modern Phys. C* **2021**, *32*, 2150050. [CrossRef]
14. Sharma, R.; Adhikari, B.; Mishra, A. Structural and spectral properties of corona graphs. *Discrete Appl. Math.* **2017**, *228*, 14–31. [CrossRef]
15. Wang, X.; Hao, Y.; Wang, Q. On the controllability of corona product network. *J. Franklin Inst.* **2020**, *357*, 6228–6240. [CrossRef]
16. Shamir, A. How to share a secret. *Comm. ACM* **1979**, *22*, 612–613. [CrossRef]
17. Blakley, G.R. Safeguarding cryptographic keys. In *Managing Requirements Knowledge*; Merwin, R., Zanca, J., Smith, M., Eds.; IEEE: New York, NY, USA, 1979; pp. 313–317.
18. Attasena, V.; Darmont, J.; Harbi, N. Secret sharing for cloud data security. *VLDB J.* **2017**, *26*, 657–681. [CrossRef]
19. Tompa, M.; Wall, H. How to share a secret with cheaters. *J. Cryptol.* **1988**, *1*, 133–138. [CrossRef]
20. Lin, H.Y.; Harn, L. Fair reconstruction of a secret. *Inf. Process. Lett.* **1995**, *55*, 45–47. [CrossRef]
21. He, J.; Dawson, E. Shared secret reconstruction. *Des. Codes Cryptogr.* **1998**, *14*, 221–237. [CrossRef]
22. Laih, C.S.; Lee, Y.C. A v-fairness (t, n) secret sharing scheme. *IEE Proc. Comput. Digit. Tech.* **1997**, *144*, 245–248. [CrossRef]
23. Hwang, R.J.; Chang, C.C. Enhancing the efficiency of (v, r, n)-fairness secret sharing scheme. In Proceedings of the 18th Internet Conference on Advanced Information Networking and Application, AINA 2004, Fukuoka, Japan, 29–31 March 2004; Barolli, L., Ed.; IEEE: Los Alamitos, CA, USA, 2004; pp. 208–212.
24. Lee, Y.C. A Simple (v, t, n)-fairness secret sharing scheme with one shadow for each participant. In *Web Information Systems and Mining, WISM 2011*; Gong, Z., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; pp. 384–389.
25. Halpern, J.Y.; Teague, V. Rational secret sharing and multiparty computation. In *STOC'04*; Babai, L., Ed.; ACM: Chicago, IL, USA, 2004; pp. 623–632.
26. Ong, S.J.; Parkes, D.C.; Rosen, A.; Vadhan, S. Fairness with an honest minority and a rational majority. In *Theory of Cryptography, TCC 2009*; Reingold, O., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2009; pp. 36–53.
27. Tian, Y.; Peng, C.; Lin, D.; Ma, J.; Jiang, Q.; Ji, W. Bayesian mechanism for rational secret sharing scheme. *Sci. China Inform. Sci.* **2015**, *58*, 1–13. [CrossRef]
28. Zhang, E.; Yuan, P.; Du, J. Verifiable rational secret sharing scheme in mobile networks. *Mobile Inform. Syst.* **2015**, *2015*, 462345. [CrossRef]
29. Harn, L.; Lin, C.; Li, Y. Fair secret reconstruction in (t, n)-secret sharing. *J. Inf. Secur. Appl.* **2015**, *23*, 1–7. [CrossRef]
30. Pilaram, H.; Eghlidos, T. An efficient lattice based multi-stage secret sharing scheme. *IEEE Trans. Dependabl.Secur. Comput.* **2017**, *14*, 2–8. [CrossRef]
31. Zhang, E.; Zhu, J.Z.; Li, G.L.; Chang, J.; Li, Y. Outsourcing hierarchical threshold secret sharing scheme based on reputation. *Secur. Commun. Netw.* **2019**, *2019*, 6989383. [CrossRef]
32. Zhang, E.; Li, M.; Yiu, S.M.; Du, J.; Zhu, J.Z.; Jin, G.G. Fair hierarchical secret sharing scheme based on smart contract. *Inf. Sci.* **2021**, *546*, 166–176. [CrossRef]
33. Naor, M.; Roth, R.M. Optimal file sharing in distributed networks. In Proceedings of the 32nd Annual Symposium of Foundations of Computer Science, San Juan, Puerto Rico, 1–4 October 1991; Papadimitriou, C., Ed.; IEEE: Washington, DC, USA, 1991; pp. 515–525.
34. Sardari, M.; Restrepo, R.; Fekri, F.; Soljanin, E. Memory allocation in distributed storage networks. In Proceedings of the 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; Aazhang, B., Ed.; IEEE, Piscataway, NJ, USA, 2010; pp. 1958–1962.
35. Zhang, X.; Xu, M.; Da, G.; Zha, P. Ensuring confidentiality and availability of sensitive data over a network system under cyber threats. *Reliab. Eng. Syst. Saf.* **2021**, *214*, 107697. [CrossRef]
36. Ogiela, L.; Ogiela, M.R.; Ko, H. Intelligent data management and security in cloud computing. *Sensors* **2020**, *20*, 3458. [CrossRef]
37. Lai, H.J.; Montgomery, B.; Poon, H. Upper bounds of dynamic chromatic number. *Ars Combin.* **2003**, *68*, 193–201.
38. Montgomery, B. Dynamic Coloring of Graphs. Ph.D. Thesis, West Virginia University, Ann Arbor, MI, USA, 2001.
39. Kim, J.; Ok, S. Dynamic choosability of triangle-free graphs and sparse random graphs. *J. Graph Theory* **2017**, *87*, 347–355. [CrossRef]
40. Kristiana, A.I.; Utoyo, M.I.; Alfarisi, R.; Dafik, D. r-dynamic coloring of the corona product of graphs. *Discrete Math. Algorithms Appl.* **2020**, *12*, 2050019. [CrossRef]
41. Aparna, V; Mohanapriya, N. On r-dynamic coloring of neighborhood corona of path with some graphs. *J. Phys. Conf. Ser.* **2020**, *1523*, 012001. [CrossRef]
42. Nandini, G.; Venkatachalam, M.; Falcón, R.M. On the r-dynamic coloring of subdivision-edge coronas of a path. *AIMS Math.* **2020**, *5*, 4546–4562. [CrossRef]
43. Aparna, V.; Mohanapriya, N. r-dynamic chromatic number of extended neighborhood corona of complete graph with some graphs. In *Mathematical Modelling and Computational Intelligence Techniques, ICMMCIT 2021*; Balasubramaniam, P., Ed.; Springer Proceedings in Mathematics and Statistics; Springer: Singapore, 2022; pp. 235–254.
44. Harary, F. *Graph Theory*; Addison Wesley: Reading, MA, USA, 1969.
45. Frucht, R.; Harary, F. On the corona of two graphs. *Aequationes Math.* **1970**, *4*, 322–325. [CrossRef]

46. Indulal, G. The spectrum of neighborhood corona of graphs. *Kragujevac J. Math.* **2011**, *35*, 493–500.
47. Adiga, C.; Rakshith, B.R.; Subba Krishna, K.N. Spectra of extended neighborhood corona and extended corona of two graphs. *Electron. J. Graph Theory Appl.* **2016**, *4*, 101–110. [CrossRef]
48. Lai, H.J.; Lin, J.; Montgomery, B.; Shui, T.; Fan, S. Conditional colorings of graphs. *Discrete Math.* **2006**, *306*, 1997–2004. [CrossRef]