entropy

MDPI

*Article*

# Graphic Groups, Graph Homomorphisms, and Graphic Group Lattices in Asymmetric Topology Cryptography

**Meimei Zhao [1,*], Hongyu Wang [2] and Bing Yao [3]**

[1] College of Science, Gansu Agricultural University, Lanzhou 730070, China
[2] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
[3] College of Mathematics and Statistics, Northwest Normal University, Lanzhou 730070, China
* Correspondence: zhaomeimei125@163.com

**Abstract:** Using asymmetric topology cryptography to encrypt networks on the basis of topology coding is a new topic of cryptography, which consists of two major elements, i.e., topological structures and mathematical constraints. The topological signature of asymmetric topology cryptography is stored in the computer by matrices that can produce number-based strings for application. By means of algebra, we introduce every-zero mixed graphic groups, graphic lattices, and various graph-type homomorphisms and graphic lattices based on mixed graphic groups into cloud computing technology. The whole network encryption will be realized by various graphic groups.

**Keywords:** graphic group; mixed graphic group lattice; graphic coloring; graph homomorphism; graphic category; network encryption



**Citation:** Zhao, M.; Wang, H.; Yao, B. Graphic Groups, Graph Homomorphisms, and Graphic Group Lattices in Asymmetric Topology Cryptography. *Entropy* **2023**, *25*, 720. https://doi.org/10.3390/e25050720

Academic Editor: Kinkar Chandra Das

Received: 23 February 2023
Revised: 12 April 2023
Accepted: 21 April 2023
Published: 26 April 2023



## 1. Introduction

### 1.1. Research Background

Cryptography is the core technology and basic support to ensure network and information security. As is well known, modern cryptography and its mathematical theories, such as lattice cryptography, are used as a kind of cryptography to resist quantum computing attacks. From Ref. [1], one can learn more about the importance and research status of lattice cryptography in the design of mathematical problems as well as its development and applications.

Xiaogang Wen, an academician of the United States, pointed out in his article entitled "New revolution in physics modern mathematics in condensed matter physics" that "But since the quantum revolution, especially, the second quantum revolution, we are more and more aware that our world is not continuous, but discrete. We should look at the world from the perspective of algebra." Indeed, the development of modern mathematics proceeds exactly from continuous to discrete as well as from analysis to algebra. Modern mathematics also asserts the notion that discrete algebra is more essential than continuous analysis.

Group theory and, in particular, non-Abelian groups provide plenty of supply of complex and varied problems for cryptography. Over the past few decades, group-based cryptography has been extensively studied. For example, in 1999 Anshel and coauthors proposed the commutator key-exchange protocol based on the braid groups [2]. In 2004, Eick and Kahrobaei proposed the polycyclic groups as a new platform for cryptography [3]. These polycyclic groups are a natural generalization of cyclic groups with more complex algorithmic theory. In 2008, Ostrovsky and Skeith III determined sufficient and necessary conditions for the existence of a fully homomorphic encryption scheme (over a non-zero ring) if and only if homomorphic encryption exists over any finite non-Abelian simple group [4]. Since 2016, graph groups have been proposed by Flores, Kahrobaei, and Koberda for various cryptographic protocols as several of the algorithmic problems in these graph groups are NP-complete, which provides quantum-resistant cryptosystems (see, Section 7 of

Ref. [5] for more detail). Moreover, in 2019 Kahrobaei and coauthors proposed the nilpotent groups for making multi-linear maps [6]. In 2021, Anshel and coauthors presented the so-called WalnutDSA™ [7], a group-based quantum-resistant public-key digital signature method on the basis of the one-way function E-multiplication. It can provide very efficient means of validating digital signatures, as the authors claimed [7], which is essential for low-powered and constrained devices. Just very recently, a complete overview of the actual state of group-based cryptography in the quantum era was updated by Kahrobaei, Flores, and Noce [8], in which some important encryption groups such as polycyclic groups and graph groups, as well as relevant combinatorial algebraic problems, are reviewed in detail.

The advantages of asymmetric encryption are as follows: higher security, the public key is public, and the private key is saved by oneself instead of sharing with others. In Ref. [9], we proposed the graphic group based on the Abelian additive operation of finite modulus in 2017, called *every-zero graphic group*. Graphic groups were further investigated in detail [10–14]. The mixed graphic group was introduced for the first time in Ref. [15] and then employed to encrypt networks in whole. Moreover, the infinite graphic group was also introduced [16].

Cryptographical graphs should possess the following characteristics: (1) they can be conveniently used in daily activities; (2) they are characterized by strong security, i.e., they are difficult to crack; (3) graphs and colorings (resp. labelings) are available for making topological key-pairs. In the present work, our goal is to propose some techniques of asymmetric topology cryptography for encrypting networks.

The present paper is structured as follows. After introducing basic concepts and definitions in Section 1.2, in the following section we shall focus on graphic groups by introducing mixed graphic groups and some particular mixed graphic groups such as infinite mixed graphic groups and their homomorphisms. In Section 3, some graphic lattices will be built up by several every-zero mixed graphic groups for encrypting networks. In Section 4, we will discuss the whole network encryption, such as encrypting tree-like networks.

### *1.2. Basic Concepts and Definitions*

In the present paper, the terminologies and notations from Refs. [17–19], as well as the following notations, will be used.

Throughout this paper, let $G$ be a non-trivial simple undirected graph with vertex set $V(G)$ and edge set $E(G)$. A graph $G$ is a $(p,q)$-*graph* if $|V(G)| = p$ and $|E(G)| = q$. A tree is a connected acyclic graph, in which a *leaf* is a vertex of degree one and any two vertices are connected by a unique path. A simple graph is called a *complete graph* if each pair of distinct vertices is joined by an edge in the graph. A complete graph of $n$ vertices is denoted as $K_n$. A *bipartite graph* $H$ holds $V(H) = X \cup Y$ with $X \cap Y = \emptyset$ such that each edge $uv \in E(H)$ holds $u \in X$ and $v \in Y$.

The cardinality of a set $X$ is denoted as $|X|$; $[a,b]$ indicates a set $\{a, a+1, a+2, \ldots, b\}$ with integers $a, b$ holding $a < b$; $[r,s]^o$ denotes an odd-integer set $\{r, r+2, \ldots, s\}$ with odd numbers $r, s$ holding $1 \leq r \leq s-2$ true; and $Z^0$ represents the set of all non-negative integers.

A graph labeling is an assignment of integers to the vertices or edges, or both, subject to certain conditions. In fact, graph labeling was first introduced in the mid 1960s, and since then approximately 200 graph-labeling techniques have been investigated [20]. In addition, the statement "a $W$-constraint proper total coloring (resp. labeling)" means one of various graph labelings, or one of various graph colorings hereafter. Graph colorings and labelings that are not defined here can be found in Refs. [20,21]. Motivated by the algebraic category, here we propose the graphic category as follows:

**Definition 1.** *A graphic category* $\boldsymbol{G}$ *consists of*

*(i) A set of graphs admitting total colorings;*

*(ii) A set of morphisms from* $A$ *to* $B$ *for two graphs* $A, B \in \boldsymbol{G}$*, which is denoted as* $H_{om}(A, B)$*. For two morphisms* $f \in H_{om}(A, B)$ *and* $g \in H_{om}(B, C)$*, the morphism* $g \circ f \in H_{om}(A, C)$ *is called composition, and it satisfies the following two axioms:*

*(1)* ***Associativity law****. For morphisms* $f \in H_{om}(A, B)$*,* $g \in H_{om}(B, C)$*, and* $h \in H_{om}(C, D)$*, we have* $(h \circ g) \circ f = h \circ (g \circ f)$*;*

*(2)* ***Identity law****. For any morphism* $f \in H_{om}(A, B)$*, we have* $f \circ 1_A = f = 1_B \circ f$*, where* $1_A \in H_{om}(A, A)$ *and* $1_B \in H_{om}(B, B)$*.*

**Definition 2.** *A set* $S$ *of graphs* $S_i$ *admitting X-constraint total colorings* $f_i$ *is called the X-constraint every-zero mixed graphic group, if there is an Abelian additive operation "*$[+_k]$*" on the elements of* $S$ *in the following way: arbitrarily take an element* $S_k \in S$ *as the* zero*. We define the operation* $S_i[+_k]S_j$ *as follows:*

$$S_i[+_k]S_j := S_i[+]S_j[-]S_k = S_\lambda \in S \tag{1}$$

*with* $\lambda = i + j - k \pmod{\varepsilon}$ *computed by*

$$f_i[+_k]f_j := \big[f_i(\omega) + f_j(\omega) - f_k(\omega)\big] \pmod{\varepsilon} = f_\lambda(\omega) \tag{2}$$

*with* $f_\lambda(\omega) \in f_\lambda(V(S) \cup E(S))$ *and any preappointed zero* $S_k \in S$*.*

**Definition 3** (See also Ref. [22])**.** *Suppose that a* $(p, q)$*-graph* $G$ *admits a W-constraint total coloring* $f : V(G) \cup E(G) \to [a, b]$*; a colored Topcode-matrix* $T_{code}(G, f)$ *of the graph* $G$ *is defined as*

$$T_{code}(G, f) = \begin{pmatrix} f(x_1) & f(x_2) & \cdots & f(x_q) \\ f(x_1y_1) & f(x_2y_2) & \cdots & f(x_qy_q) \\ f(y_1) & f(y_2) & \cdots & f(y_q) \end{pmatrix}_{3\times q} = \begin{pmatrix} X_f \\ E_f \\ Y_f \end{pmatrix} = (X_f, E_f, Y_f)^T \tag{3}$$

*holding the W-constraint* $W\langle f(x_i), f(x_iy_i), f(y_i)\rangle = 0$ *for* $i \in [1, q]$*. Moreover, if* $G$ *is a bipartite graph with the vertex set* $V(G) = X^v \cup Y^v$ *and* $X^v \cap Y^v = \emptyset$*, we stipulate* $x_i \in X^v$ *and* $y_i \in Y^v$ *such that* $X_f \cap Y_f = \emptyset$ *in Equation (3), where "W-constraint" is a mathematical constraint, or a group of mathematical constraints.*

## 2. Graphic Groups

### *2.1. Mixed Graphic Groups*

Wang et al. have defined the *mixed graphic group* [15]; here, we present an improved definition of the mixed graphic group as follows:

**Definition 4.** *Suppose that a* $(p, q)$*-graph* $G$ *admits a W-constraint proper total coloring* $f : V(G) \cup E(G) \to [1, M]$*, such that two color sets* $f(V(G)) = \{f(x) : x \in V(G)\}$ *and* $f(E(G)) = \{f(uv) : uv \in E(G)\}$ *hold a collection of restrictions. We define a colored graph set* $M_f(G) = \{G_{s,k} : s \in [1, p], k \in [1, q]\}$ *with* $G_{s,k} \cong G$*, we define a W-constraint proper total coloring* $g_{s,k}(x) = f(x) + s \pmod{p}$ *for every vertex* $x \in V(G_{s,k})$*, and* $g_{s,k}(uv) = f(uv) + k \pmod{q}$ *for each edge* $uv \in E(G_{s,k})$*.*

**Lemma 1.** *Each colored graph set* $M_f(G)$ *defined in Definition 4 forms an every-zero mixed graphic group based on the Abelian additive operation defined in Definition 2.*

**Proof.** By Definitions 2 and 4, we define the Abelian additive operation "$G_{s,k}[+_{a,b}]G_{i,j}$" on the colored graph set $M_f(G)$ under a preappointed zero $G_{a,b} \in M_f(G)$ as follows,

$$\big[g_{s,k}(w) + g_{i,j}(w) - g_{a,b}(w)\big] \pmod{\varepsilon} = g_{\lambda,\mu}(w) \in M_f(G) \tag{4}$$

for each element $w \in V(G) \cup E(G)$, where $\lambda = s + i - a \pmod p$ and $\mu = k + j - b \pmod q$. As $w = x \in V(G)$, we have $\varepsilon = p$, and thus Equation (4) is equivalent to

$$\left[g_{s,k}(x) + g_{i,j}(x) - g_{a,b}(x)\right] \pmod p = g_{\lambda,\mu}(x) \in M_f(G). \tag{5}$$

As $w = uv \in E(G)$, we have $\varepsilon = q$, and Equation (4) is also equivalent to

$$\left[g_{s,k}(uv) + g_{i,j}(uv) - g_{a,b}(uv)\right] \pmod q = g_{\lambda,\mu}(uv) \in M_f(G). \tag{6}$$

Especially, as $s = i = a = \alpha$, we have mod $\varepsilon$ = mod $q$ in Equation (4), and thus we obtain

$$\left[g_{\alpha,k}(uv) + g_{\alpha,j}(uv) - g_{\alpha,b}(uv)\right] \pmod q = g_{\alpha,\mu}(uv) \in M_f(G) \tag{7}$$

for $uv \in E(G)$. When $k = j = b = \beta$, and mod $\varepsilon$ = mod $p$ in Equation (4), we have

$$\left[g_{s,\beta}(x) + g_{i,\beta}(x) - g_{a,\beta}(x)\right] \pmod p = g_{\lambda,\beta}(x) \in M_f(G) \tag{8}$$

for $x \in V(G)$.

We show the following facts on the colored graph set $M_f(G)$:

(i) *Zero.* Each graph $G_{a,b} \in M_f(G)$ can be determined as *zero* such that $G_{s,k}[+_{a,b}]G_{a,b} = G_{s,k}$.

(ii) *Uniqueness.* For $G_{s,k}[+_{a,b}]G_{i,j} = G_{c,d} \in M_f(G)$ and $G_{s,k}[+_{a,b}]G_{i,j} = G_{r,t} \in M_f(G)$, we have the facts $c = s + i - a \pmod p = r$ and $d = k + j - b \pmod q = t$ under the zero $G_{a,b}$.

(iii) *Inverse.* Each graph $G_{s,k} \in M_f(G)$ has its own *inverse* $G_{s',k'} \in M_f(G)$ holding $G_{s,k}[+_{a,b}]G_{s',k'} = G_{a,b}$ determined by $\left[g_{s,k}(w) + g_{s',k'}(w)\right] \pmod \varepsilon = 2g_{a,b}(w)$ for each element $w \in V(G) \cup E(G)$.

(iv) *Associative law.* Under the zero $G_{a,b}$, each triple $G_{s,k}, G_{i,j}, G_{c,d} \in M_f(G)$ holds

$$G_{s,k}[+_{a,b}]\left(G_{i,j}[+_{a,b}]G_{c,d}\right) = \left(G_{s,k}[+_{a,b}]G_{i,j}\right)[+_{a,b}]G_{c,d}$$

(v) *Commutative law.* Each pair of $G_{s,k}, G_{i,j} \in M_f(G)$ holds $G_{s,k}[+_{a,b}]G_{i,j} = G_{i,j}[+_{a,b}]G_{s,k}$ under the zero $G_{a,b}$.

The proof of the lemma is complete. □

**Remark 1.** *Regarding the proof of Lemma 1, there are*

*(i) By Equations (5) and (6) shown in the proof of Lemma 1, we have*

$$\left[f(x) + s + f(x) + i - (f(x) + a)\right] \pmod p = f(x) + s + i - a \pmod p = g_{\lambda,\mu}(x) \tag{9}$$

*with* $\lambda = s + i - a \pmod p$, *and*

$$\left[f(uv) + k + f(uv) + j - (f(uv) + b)\right] \pmod q = f(uv) + k + j - b \pmod q = g_{\lambda,\mu}(uv) \tag{10}$$

*with* $\mu = k + j - b \pmod q$. *Thus, we obtain a formula*

$$G_{s,k}[+]G_{i,j}[-]G_{a,b} = G_{\lambda,\mu} \in M_f(G). \tag{11}$$

*(ii) We call the mixed graphic group* $M_f(G) = \{G_{s,k} : s \in [1,p], k \in [1,q]\}$ *every-zero mixed graphic group based on the Abelian additive operation "*$G_{i,j}[+_{a,b}]G_{s,k}$*" defined in Equation (4), denote it as* $\boldsymbol{G} = \{M_f(G); [+]\}$, *and we present its matrix expression as follows:*

$$\boldsymbol{G} = \begin{pmatrix} G_{1,1} & G_{1,2} & \cdots & G_{1,q} \\ G_{2,1} & G_{2,2} & \cdots & G_{2,q} \\ \cdots & \cdots & \cdots & \cdots \\ G_{p,1} & G_{p,2} & \cdots & G_{p,q} \end{pmatrix}_{p \times q} \tag{12}$$

*(iii) The every-zero mixed graphic group* $\boldsymbol{G}$ *contains* $pq$ *graphs in total. There are two particular every-zero graphic subgroups,* $\{F_v(G);[+]\} = \{G_{s,1} : s \in [1,p]\} \subset \boldsymbol{G}$ *and* $\{F_e(G);[+]\} = \{G_{1,k} : k \in [1,q]\} \subset \boldsymbol{G}$*, based on the Abelian additive operation. In fact,* $\boldsymbol{G}$ *contains at least* $(p+q)$ *every-zero graphic subgroups.*

Figure 1 shows an every-zero mixed graphic group based on a colored graph set $M_f(G) = \{G_{s,k} : s \in [1,6], k \in [1,5]\}$, where $6 = 0 \pmod 6$ and $5 = 5 \pmod 5$ for vertex colors, whereas $5 = 0 \pmod 5$ for edge colors. By using the colored graphs shown in Figure 1, one can readily verify Equation (11): $G_{s,k}[+]G_{i,j}[-]G_{a,b} = G_{\lambda,\mu}$ for vertices and edges.

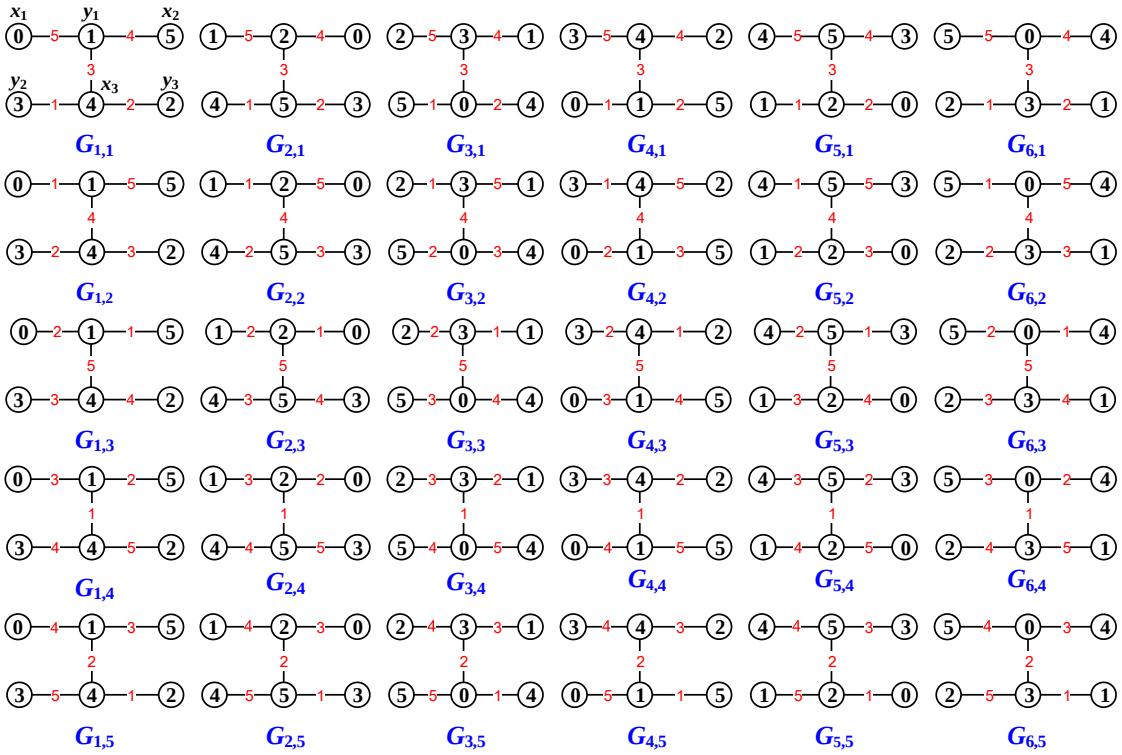



**Figure 1.** An every-zero mixed graphic group $\boldsymbol{G}$ for illustrating Definition 4 and Lemma 1.

**Theorem 1.** *Each every-zero mixed graphic group* $\boldsymbol{G} = \{M_f(G);[+]\}$ *defined in Remark 1; Definitions 3 and 4 form a graphic category based on a preappointed zero* $G_{a,b} \in \boldsymbol{G}$ *defined in Definition 1.*

**Proof.** We define a *graphic morphism* $\theta_{a,b}(G_{s,k}, G_{i,j})$ from $G_{s,k}$ to $G_{i,j}$ by the Abelian additive operation $G_{s,k}[+_{a,b}]G_{i,j}$ based on a preappointed zero $G_{a,b} \in \boldsymbol{G} = \{M_f(G);[+]\}$, that is, $\theta_{a,b}(G_{s,k}, G_{i,j}) := G_{s,k}[+_{a,b}]G_{i,j}$. Notice that $G_{s,k}[+_{a,b}]G_{i,j} = G_{i,j}[+_{a,b}]G_{s,k}$, so $\theta_{a,b}(G_{s,k}, G_{i,j}) = \theta_{a,b}(G_{i,j}, G_{s,k})$.

For $G_{i,j}, G_{i+1,j+1}, G_{i+2,j+2} \in \boldsymbol{G}$, we define the composition of two graphic morphisms as follows:

$$\begin{aligned} \theta_{a,b}(G_{i,j}, G_{i,j+2}) &= \theta_{a,b}(G_{i,j}, G_{i,j+1}) \circ \theta_{a,b}(G_{i,j+1}, G_{i,j+2}) \\ &= \left(G_{i,j}[+_{a,b}]G_{i,j+1}\right) \circ \left(G_{i,j+1}[+_{a,b}]G_{i,j+2}\right) \\ &= G_{i,j}[+_{a,b}]G_{i,j+2} \end{aligned} \tag{13}$$

and

$$\begin{aligned}\theta_{a,b}(G_{i,j}, G_{i+2,j}) &= \theta_{a,b}(G_{i,j}, G_{i+1,j}) \circ \theta_{a,b}(G_{i+1,j}, G_{i+2,j}) \\ &= \left(G_{i,j}[+_{a,b}]G_{i+1,j}\right) \circ \left(G_{i+1,j}[+_{a,b}]G_{i+2,j}\right) \\ &= G_{i,j}[+_{a,b}]G_{i+2,j}.\end{aligned} \tag{14}$$

So, we have

$$\begin{aligned}\theta_{a,b}(G_{i,j}, G_{i+2,j+2}) &= \theta_{a,b}(G_{i,j}, G_{i+1,j+1}) \circ \theta_{a,b}(G_{i+1,j+1}, G_{i+2,j+2}) \\ &= \left(G_{i,j}[+_{a,b}]G_{i+1,j+1}\right) \circ \left(G_{i+1,j+1}[+_{a,b}]G_{i+2,j+2}\right) \\ &= G_{i,j}[+_{a,b}]G_{i+2,j+2}.\end{aligned} \tag{15}$$

Since $\theta_{a,b}(G_{s,k}, G_{i,j}) \circ 1_{s,k} = \theta_{a,b}(G_{s,k}, G_{i,j})$ for $1_{s,k} = \theta_{a,b}(G_{s,k}, G_{s,k})$ and $1_{i,j} \circ \theta_{a,b}(G_{s,k}, G_{i,j}) = \theta_{a,b}(G_{s,k}, G_{i,j})$ for $1_{i,j} = \theta_{a,b}(G_{i,j}, G_{i,j})$, the identity law in Definition 1 holds true. The associativity law stands for graphic morphisms.

In general, by using Equations (13) and (14) repeatedly, we can obtain a *graphic morphism composition* as follows:

$$\begin{aligned}\theta_{a,b}(G_{i,j}, G_{s,k}) &= \theta_{a,b}(G_{i,j}, G_{c,d}) \circ \theta_{a,b}(G_{c,d}, G_{s,k}) \\ &= \left(G_{i,j}[+_{a,b}]G_{c,d}\right) \circ \left(G_{c,d}[+_{a,b}]G_{s,k}\right) \\ &= G_{i,j}[+_{a,b}]G_{s,k}\end{aligned} \tag{16}$$

and the *graphic morphism triangular law*.

We claim that the every-zero mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ forms a graphic category based on the graphic morphism set $H_{om}^{a,b}(G_{i,j}, G_{s,k}) = \{\theta_{a,b}(G_{i,j}, G_{s,k}) : G_{i,j}, G_{s,k} \in \boldsymbol{G}\}$ for the preappointed zero $G_{a,b} \in \boldsymbol{G}$. □

**Theorem 2.** *Each every-zero mixed graphic group* $\boldsymbol{G} = \{M_f(G); [+]\}$ *defined in Definitions 3 and 4 forms m graphic categories such as* $H_{om}^{a,b}(G_{i,j}, G_{s,k})$, *shown in the proof of Theorem 1, for each* $G_{a,b} \in \boldsymbol{G}$ , *where m is the number of elements of the every-zero mixed graphic group* $\boldsymbol{G}$.

**Theorem 3.** *A Topcode-matrix group* $\{T_{code}(G_{s,k}, g_{s,k}) : G_{s,k} \in \boldsymbol{G} = \{M_f(G); [+]\}\}$ *based on an every-zero mixed graphic group* $\boldsymbol{G} = \{M_f(G); [+]\}$ *defined in Definitions 3 and 4 forms a* Topcode-matrix category *defined in Definitions 1 and 3.*

**Remark 2.** *(i) We take three Topcode-matrices*

$$T_{code}(G_{1,2}, g_{1,2}),\ T_{code}(G_{3,3}, g_{3,3}),\ T_{code}(G_{6,4}, g_{6,4}) \in M_T = \{T_{code}(G_{s,k}, g_{s,k}) : G_{s,k} \in \{M_f(G); [+]\}\},$$

*where the Topcode-matrix set* $M_T$ *is made by the Topcode-matrices of the colored graphs of the every-zero mixed graphic group* $M_f(G) = \{G_{s,k} : s \in [1,6], k \in [1,5]\}$ *shown in Figure 1. Let* $T_{code}(G_{6,4}, g_{6,4})$ *be zero; we compute*

$$\begin{aligned}&T_{code}(G_{1,2}, g_{1,2})\ [+]\ T_{code}(G_{3,3}, g_{3,3})\ [-]\ T_{code}(G_{6,4}, g_{6,4}) \\ &= \begin{pmatrix} 0 & 1 & 1 & 3 & 4 \\ 1 & 5 & 4 & 2 & 3 \\ 1 & 5 & 4 & 4 & 2 \end{pmatrix} [+] \begin{pmatrix} 2 & 3 & 3 & 5 & 0 \\ 2 & 1 & 5 & 3 & 4 \\ 3 & 1 & 0 & 0 & 4 \end{pmatrix} [-] \begin{pmatrix} 5 & 0 & 0 & 2 & 3 \\ 3 & 2 & 1 & 4 & 5 \\ 0 & 4 & 3 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 4 & 4 & 0 & 1 \\ 5 & 4 & 3 & 1 & 2 \\ 4 & 2 & 1 & 1 & 5 \end{pmatrix} = T_{code}(G_{4,1}, g_{4,1}) \\ &= \begin{pmatrix} g_{4,1}(x_1) & g_{4,1}(y_1) & g_{4,1}(y_1) & g_{4,1}(y_2) & g_{4,1}(x_3) \\ g_{4,1}(x_1y_1) & g_{4,1}(x_2y_1) & g_{4,1}(x_3y_1) & g_{4,1}(x_3y_2) & g_{4,1}(x_3y_3) \\ g_{4,1}(y_1) & g_{4,1}(x_2) & g_{4,1}(x_3) & g_{4,1}(x_3) & g_{4,1}(y_3) \end{pmatrix}\end{aligned} \tag{17}$$

*under the edge modular* mod 5 *and the vertex modular* mod 6. *By using the Abelian additive operation "*$T_{code}(G_{s,k}, g_{s,k})[+_{a,b}]T_{code}(G_{i,j}, g_{i,j})$*", it is not hard to verify the Topcode-matrix set* $M_T$ *forms a Topcode-matrix group.*

*(ii) From Definition 3, each Topcode-matrix* $T_{code}(G_{s,k}, g_{s,k})$ *generates* $(3q)!$ *number-based strings for real application. As can be seen from Equation (17), the Topcode-matrix* $T_{code}(G_{4,1}, g_{4,1})$ *can induce the following number-based strings:*

$$344015431242115,\ 354244432110125,\ 343124421150154$$

*for encrypting digital files of information networks.*

*(iii) Notice that a Topcode-matrix* $T_{code}(G_{s,k}, g_{s,k})$ *corresponds to two or more graphs, which are mutually not isomorphic from each other in general; see Figure 2 for examples. Coloring a connected graph with the elements of a Topcode-matrix group* $\{T_{code}(G_{s,k}, g_{s,k}) : G_{s,k} \in \boldsymbol{G}\}$ *is a new topic in the Topcode-matrix category.*

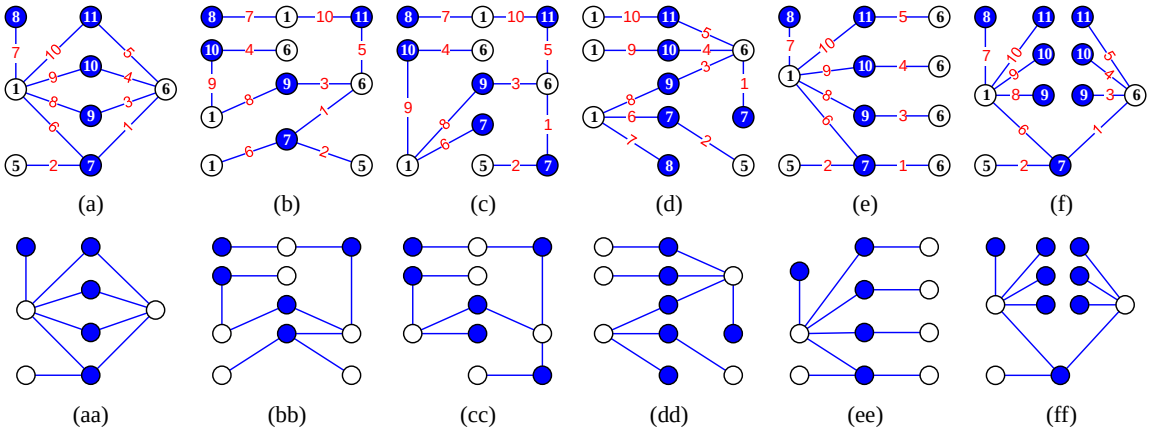



**Figure 2.** (**a**–**f**) correspond to one Topcode-matrix, but (**aa**–**ff**) are mutually not isomorphic from each other.

**Theorem 4.** *For two every-zero mixed graphic groups* $\{M_f(G); [+]\}$ *and* $\{F_h(H); [+]\}$ *defined in Remark 1, suppose that* $M_f(G) = \{G_1, G_2, \ldots, G_n\}$ *and* $F_h(H) = \{H_1, H_2, \ldots, H_n\}$, *and there are graph homomorphisms* $G_i \to H_i$ *defined by* $\theta_i : V(G_i) \to V(H_i)$ *such that each edge* $uv \in E(G_i)$ *corresponds to an edge* $\theta_i(u)\theta_i(v) \in E(H_i)$ *for* $i \in [1, n]$. *Then, we obtain an every-zero mixed graphic group homomorphism,*

$$\{M_f(G); [+]\} \to \{F_h(H); [+]\}. \tag{18}$$

### *2.2. Some Mixed Graphic Groups*

#### 2.2.1. Twin Mixed Graphic Groups

In Ref. [23], the authors introduced several matching colorings (resp. labelings) of graphs and also pointed out matching diversity: configuration matching partition, coloring matching partition, set matching partition, matching chain, one-vs.-more and more-vs.-more styles of matching partitions, configuration-vs.-configuration, configuration-vs.-labeling, labeling-vs.-labeling and (configuration, labeling)-vs.-(configuration, labeling), etc. Moreover, Wang et al. [15,24] introduced the *twin odd-graceful labelings*: Suppose $f : V(G) \to [0, 2q-1]$ is an odd-graceful labeling of a $(p, q)$-graph $G$ with $p$ vertices and $q$ edges, and $g : V(H) \to [1, 2q]$ is a labeling of another graph $H$ with $p'$ vertices and $q'$ edges such that each edge $uv \in E(H)$ has its own color defined as $g(uv) = |g(u) - g(v)|$ and the edge color set $g(E(H)) = [1, 2q-1]^o$; we say $(f, g)$ is a *twin odd-graceful labeling*, and $H$ a *twin odd-graceful matching* of $G$. Figure 3 shows some examples of the twin odd-graceful matchings.

By the notation of Remark 1, we can obtain a *twin odd-graceful mixed graphic groups* $\{M_f(G);[+]\}$ and $\{M_g(H);[+]\}$ based on a twin odd-graceful labeling $(f,g)$. Notice that $G \ncong H$, or $G \not\to H$, in general.

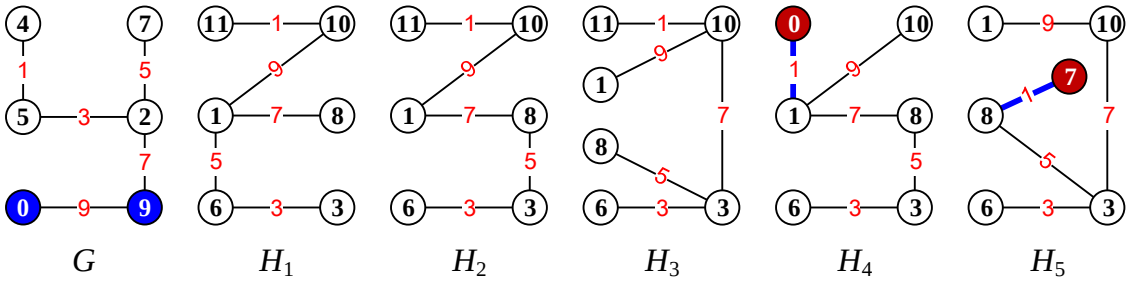



**Figure 3.** The graph $G$ admits an odd-graceful labeling, which forms a twin odd-graceful matching together with each of the graphs $H_i$ with $i \in [1,5]$.

2.2.2. Dual Mixed Graphic Groups

Suppose that a $(p,q)$-graph $G$ admits a $W$-constraint total coloring $f : V(G) \cup E(G) \to [a,b]$. Let $\max f = \max\{f(w) : w \in V(G) \cup E(G)\}$ and $\min f = \min\{f(w) : w \in V(G) \cup E(G)\}$. We call the total coloring $g(w) = \max f + \min f - f(w)$ for each element $w \in V(G) \cup E(G)$ *totally dual W-constraint total coloring* of the total coloring $f$. Notice that

$$\max g + \min g = g(w) + f(w) = \max f + \min f,\ w \in V(G) \cup E(G).$$

Then, $\{M_g(G);[+]\}$ is called a *dual mixed graphic group* of the mixed graphic group $\{M_f(G);[+]\}$ based on a pair of mutually dual $W$-constraint colorings $f$ and $g$. Notice that these two mixed graphic groups are built up on the same graph $G$.

Respectively, we call

(i) $\alpha(x) = \max f_v + \min f_v - f(x)$ for each vertex $x \in V(G)$ and $\alpha(uv) = f(uv)$ for each edge $uv \in E(G)$ *vertex-dual W-constraint coloring* of $G$, where $\max f_v = \max\{f(x) : x \in V(G)\}$ and $\min f_v = \min\{f(x) : x \in V(G)\}$;

(ii) $\beta(uv) = \max f_e + \min f_e - f(uv)$ for each edge $uv \in E(G)$ and $\beta(x) = f(x)$ for each vertex $x \in V(G)$ *edge-dual W-constraint coloring* of $G$, where $\max f_e = \max\{f(uv) : uv \in E(G)\}$ and $\min f_e = \min\max\{f(uv) : uv \in E(G)\}$;

(iii) $(\alpha,\beta)$ defined in (i) and (ii) *ve-separately dual W-constraint coloring* of the total coloring $f$.

Figure 4 shows some examples for illustrating the four dual colorings mentioned above.

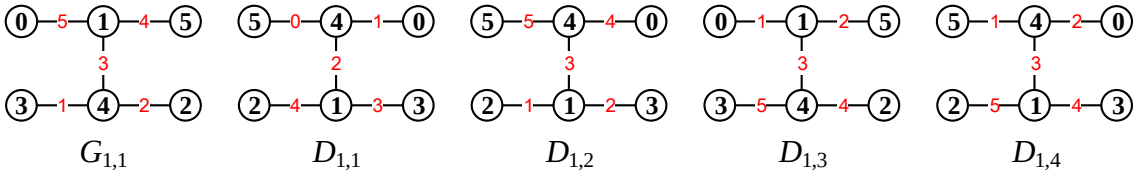



**Figure 4.** Examples for illustrating four dual colorings.

2.2.3. Matching Mixed Graphic Groups

If a $(p,q)$-graph $G$ is bipartite and admits a set-ordered graceful labeling $f$, there is a dozen of labelings $g_i$ equivalent to $f$ [21,25], and thus we obtain a dozen *matching mixed graphic groups* $\{M_f(G);[+]\}$ and $\{F_{g_i}(H_i);[+]\}$ with $i \in [1,m]$ for $m \geq 2$. For example, these labelings $g_i$ are odd-graceful labeling, odd-elegant labeling, edge-magic total labeling, image-labeling, 6C-labeling, odd-6C-labeling, even-odd separable 6C-labeling, and so on (see Ref. [23] for details). Here, we refer to the mixed graphic group $\{M_f(G);[+]\}$ as a

*private-key*, and each mixed graphic group $\{F_{g_i}(H_i);[+]\}$ with $i \in [1,m]$ as a *public-key* in encrypting networks.

The complement $\overline{G}$ of a simple graph $G$ is the simple graph with vertex set $V(G)$, and two vertices are adjacent in $\overline{G}$ if and only if they are not adjacent in $G$. So, we have $\{M_f(G);[+]\}$ and $\{M_g(\overline{G});[+]\}$ as a pair of matching mixed graphic groups, where $\overline{G}$ admits a $W$-constraint coloring $g$. In general, for a graph $L = G \cup H$ with $V(L) = V(G) = V(H)$ and $E(G) \cap E(H) = \emptyset$, we have $\{M_f(G);[+]\}$ and $\{F_h(H);[+]\}$ as a pair of matching mixed graphic groups based on the graph $L = G \cup H$, where $H$ admits a $W$-constraint coloring $h$.

Figure 5 shows the complementary graph of a given graph $G_1$ and some labellings generated from a given set-ordered graceful labelling $f_1$ of the graph $G_1$.

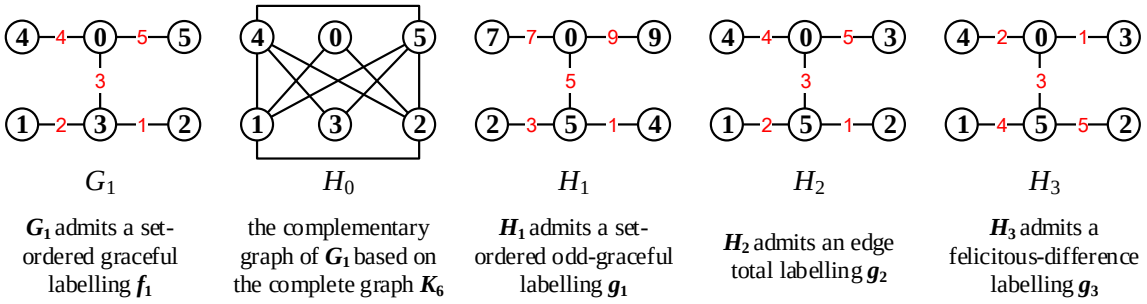



**Figure 5.** Examples of the complementary graph and three colorings $g_1, g_2, g_3$ generated from the coloring $f_1$ of $G_1$ by equivalent transformation.

### *2.3. Infinite Mixed Graphic Groups and Their Homomorphisms*

From Definition 4, we obtain an *every-zero infinite mixed graphic group*

$$\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+]) = \{G_{s,k} : -\infty < s,k < +\infty\} \tag{19}$$

with $G_{s,k} \cong G$ based on a $(p,q)$-graph $G$ admitting a $W$-constraint proper total coloring $f$ and $G \cong G_{0,0}$, where "$[+]$" is the Abelian additive operation "$G_{s,k}[+_{a,b}]G_{i,j}$" under a preappointed zero $G_{a,b} \in \boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ for any pair of graphs $G_{s,k}, G_{i,j} \in \boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$.

**Remark 3.** *The elements of an every-zero infinite mixed graphic group $\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ defined in Equation (19) can fully tile each integer point $(x,y)$ of the xOy-plane. Moreover, $\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ contains infinite every-zero mixed graphic groups having finite elements, such as $F(\{G_{s+i,k}\}_{i=1}^{p};[+])$ and $F(\{G_{s,k+j}\}_{j=1}^{q};[+])$. Additionally, $\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ contains infinite every-zero mixed graphic groups having infinite elements.*

*$\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ is also a graphic category under the graphic morphism composition defined in Equation (16). Particular every-zero mixed graphic groups having infinite elements, or finite elements can be used easily to randomly encrypt networks.*

**Theorem 5.** *(i) Suppose that the coloring $f$ of the $(p,q)$-graph $G$ based on an every-zero infinite mixed graphic group $\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+])$ is equivalent to another $W_g$-constraint total coloring $g$ of the $(p,q)$-graph $G$ based on an every-zero infinite mixed graphic group $\boldsymbol{I}_{-\infty}^{+\infty}(G,g;[+])$. If a mapping $\varphi : V(G) \cup E(G) \to V(G) \cup E(G)$ exists such that $g(w) = \varphi(f(w))$ for $w \in V(G) \cup E(G)$, then we obtain an every-zero infinite mixed graphic group homomorphism,*

$$\boldsymbol{I}_{-\infty}^{+\infty}(G,f;[+]) \to \boldsymbol{I}_{-\infty}^{+\infty}(G,g;[+]). \tag{20}$$

*(ii) Suppose a graph homomorphism from a $(p,q)$-graph $G$ to a connected graph $H$ based on a mapping $\varphi : V(G) \to V(H)$ such that each edge $uv \in E(G)$ corresponds to an edge $\varphi(u)\varphi(v) \in E(H)$, and vice versa. Suppose that the $(p,q)$-graph $G$ admits a $W$-constraint total coloring $f$, and*

*the graph $H$ admits a $W'$-constraint total coloring $h$. Then, we obtain an every-zero infinite mixed graphic group homomorphism as follows:*

$$\boldsymbol{I}_{-\infty}^{+\infty}(G, f; [+]) \to \boldsymbol{I}_{-\infty}^{+\infty}(H, h; [+]). \tag{21}$$

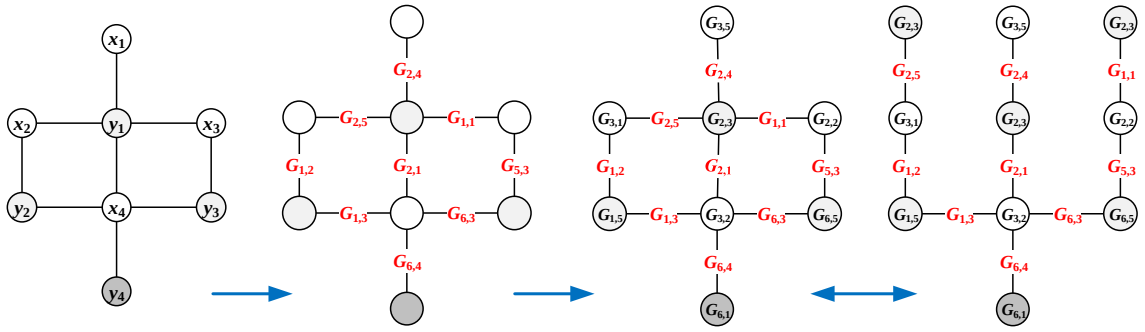
*Notice that, in general, $G \ncong H$.*

## 3. Graphic Lattices

### 3.1. Mixed Graphic $\boldsymbol{B}$-Group Lattices

**Definition 5.** *Using an every-zero mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1 to encrypt a connected graph $H$ by a mapping $\varphi : V(H) \cup E(H) \to \boldsymbol{G}$ such that each edge $uv \in E(H)$ holds $\varphi(uv) = \varphi(u)[+_{a,b}]\varphi(v)$ under a preappointed zero $G_{a,b} \in \boldsymbol{G}$, we obtain another graph $L$ from the set $\{\varphi(x), \varphi(uv) : x \in V(H), uv \in E(H)\}$ by joining some vertices of the graphs $G_{i_u,j_u} = \varphi(u) \in \boldsymbol{G}$ and $G_{i_v,j_v} = \varphi(v) \in \boldsymbol{G}$ together with some vertices of the graph $G_{i_{uv},j_{uv}} = \varphi(uv) \in \boldsymbol{G}$ via edges, respectively.*

In Figure 6, we first use an edge coloring $\varphi$ to color the edges of the uncolored graph $H$ by the elements of the every-zero mixed graphic group $M_f(G) = \{G_{s,k} : s \in [1,6], k \in [1,5]\}$ shown in Figure 1, and then an edge-colored graph $H_1$ is obtained by expending this mixed graphic group edge coloring $\varphi$ to the vertex set $V(H)$, which is followed by the totally colored graph $H_2$. Moreover, the totally colored graph $H_3$ is a *colored graph homomorphism* to $H_2$, that is, $H_3 \to_{color} H_2$.




(a) $H$ (b) $H_1$ (c) $H_2$, zero = $G_{3,4}$ (d) $H_3$, zero = $G_{3,4}$

**Figure 6.** A graphic-group-coloring for illustrating Definition 5, where (**a**) is an uncolored graph $H$; (**b**) is an edge-colored graph $H_1$ obtained by coloring the edges of $H$ with the elements of the every-zero mixed graphic group $M_f(G) = \{G_{s,k} : s \in [1,6], k \in [1,5]\}$ shown in Figure 1; (**c**) is a totally colored graph $H_2$; and (**d**) is a tree obtained from $H_2$ by splitting some vertices of $H_2$.

From the proof of Lemma 1, we use the elements of an every-zero mixed graphic group $M_f(G) = \{G_{s,k} : s \in [1,p], k \in [1,q]\}$ based on the Abelian additive operation "$G_{i,j}[+]G_{s,k}$" defined in Equation (4) to make a *mixed graphic lattice base*, i.e.,

$$\begin{aligned} \boldsymbol{B} &= (G_{1,1}, G_{2,1}, \ldots, G_{p,1}, \ldots, G_{s,k}, \ldots, G_{p,1}, G_{p,2}, \ldots, G_{p,q}) \\ &= (B_1, B_2, \ldots, B_M), \end{aligned} \tag{22}$$

where $M = pq$.

**Definition 6.** *With the notation of Equation (22), we can write the graph $L$ in Definition 5 as $L = H[\ominus_k]_{j=1}^{M} a_j B_j$ and call the following set:*

$$\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B}) = \left\{ H[\ominus_k]_{j=1}^{M} a_j B_j : a_j \in Z^0, B_j \in \boldsymbol{B}, H \in F_{m,n} \right\} \tag{23}$$

*under a preappointed zero* $B_k \in \boldsymbol{B}$ mixed graphic group lattice *based on a mixed graphic lattice base* $\boldsymbol{B}$, *where* $\sum_{j=1}^{M} a_j \geq 1$ *and* $F_{m,n}$ *is a set of graphs with vertex number* $\leq m$ *and edge number* $\leq n$. *Moreover, we call the following set:*

$$\boldsymbol{L}(F_{m,n}[\ominus]\boldsymbol{B}) = \left\{\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B}) : H_k \in \boldsymbol{B}\right\} \tag{24}$$

mixed graphic $\boldsymbol{B}$-group lattice *since each element of the mixed graphic lattice base* $\boldsymbol{B}$ *can be referred to as zero under the Abelian additive operation.*

**Remark 4.** *Regarding Definition 5, we have*

*(i) In general, two graphs* $H[\ominus_k]_{j=1}^{M} a_j B_j$ *and* $H[\ominus_s]_{j=1}^{M} a_j B_j$ *are not isomorphic from each other for two different zeros* $B_k, B_s \in \boldsymbol{B}$.

*(ii) There are many different ways to join the graph* $G_{i_{uv},j_{uv}} = \varphi(uv)$ *with two graphs* $G_{i_u,j_u} = \varphi(u)$ *and* $G_{i_v,j_v} = \varphi(v)$ *by edges in Definition 5; in other words, the number of graphs of forming* $H[\ominus_k]_{j=1}^{M} a_j B_j$ *is two or more, see Figure 7.*

*(iii) Since two graphs* $B_k, B_s \in \boldsymbol{B}$ *form two homomorphically equivalent graph homomorphisms* $B_k \to B_s$, *we obtain the following* mixed graphic group lattice homomorphisms*:*

$$\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B}) \to \boldsymbol{L}(F_{m,n}[\ominus_s]\boldsymbol{B}) \to \boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B}). \tag{25}$$

*This technology has great potential for cloud computation in the future of quantum computing.*

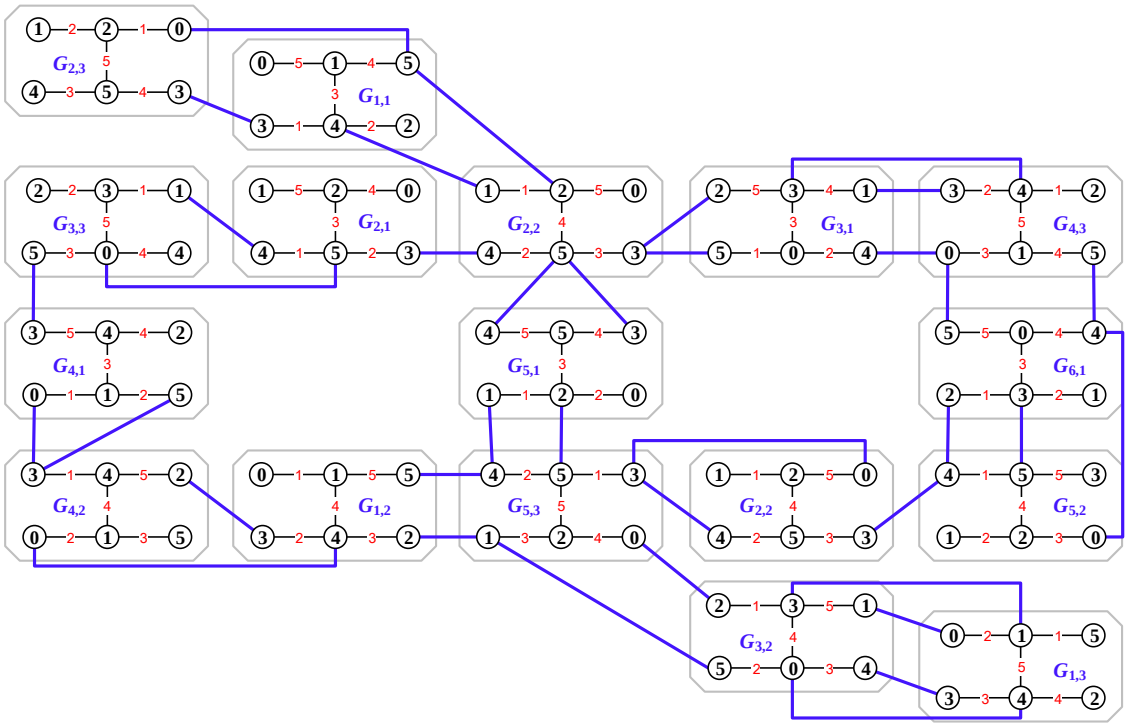



**Figure 7.** A graph $L$ for illustrating Definition 6 and Remark 4 (ii). $L$ is obtained from the totally colored graph $H_2$ shown in Figure 6 by the edge-join operation and the every-zero mixed graphic group shown in Figure 1.

### *3.2. Graphic Lattices Made by Graph Matchings*

In the following discussion, we will use traditional complementary graphs and $G$-complementary graphs to build up graphic lattices.

3.2.1. Traditional Graph and Its Complement

Let $\overline{G}$ be the *complement* of a simple graph $G$; then, we say that $(G, \overline{G})$ is a *complete-graphic matching*. For a graph operation "$(\bullet)$", we have a *complementary mixed graphic lattice*

$$\boldsymbol{L}(\overline{F}_{m,n}(\bullet)\boldsymbol{B}) = \left\{\overline{G}(\bullet)_{i=1}^{M} a_i B_i : \ a_i \in Z^0, \ B_i \in \boldsymbol{B}, \ \overline{G} \in \overline{F}_{m,n}\right\}, \tag{26}$$

where the mixed graphic lattice base $\boldsymbol{B} = (B_1, B_2, \ldots, B_M)$ is defined in Equation (22), $\overline{F}_{m,n}$ is the set of all complements of graphs of $F_{m,n}$ defined in Definition 6, and $\sum_{i=1}^{M} a_i \geq 1$.

Let $\overline{\boldsymbol{B}} = (\overline{B}_1, \overline{B}_2, \ldots, \overline{B}_M)$ be the *complementary base* of the mixed graphic lattice base $\boldsymbol{B}$ with the complement $\overline{B}_i$ of $B_i$ for $i \in [1, M]$. We obtain a *complementary mixed graphic lattice*

$$\boldsymbol{L}(F_{m,n}(\bullet)\overline{\boldsymbol{B}}) = \left\{G(\bullet)_{i=1}^{M} a_i \overline{B}_i : \ a_i \in Z^0, \ \overline{B}_i \in \overline{\boldsymbol{B}}, \ G \in F_{m,n}\right\} \tag{27}$$

with $\sum_{i=1}^{M} a_i \geq 1$. Moreover, we obtain a *totally complementary mixed graphic lattice* as follows:

$$\boldsymbol{L}(\overline{F}_{m,n}(\bullet)\overline{\boldsymbol{B}}) = \left\{\overline{G}(\bullet)_{i=1}^{M} a_i \overline{B}_i : \ a_i \in Z^0, \ \overline{B}_i \in \overline{\boldsymbol{B}}, \ \overline{G} \in \overline{F}_{m,n}\right\} \tag{28}$$

with $\sum_{i=1}^{M} a_i \geq 1$.

We call $\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B})$ and $\boldsymbol{L}(\overline{F}_{m,n}(\bullet)\overline{\boldsymbol{B}})$ a matching of *complementary mixed graphic lattices*. However, for each graph $G^* = G(\bullet)_{i=1}^{M} a_i B_i$ of $\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B})$, the complementary graph $\overline{G^*}$ of $G^*$ is not a graph $\overline{G}(\bullet)_{i=1}^{M} a_i \overline{B}_i$ of $\boldsymbol{L}(\overline{F}_{m,n}(\bullet)\overline{\boldsymbol{B}})$, in general.

3.2.2. $G$-Complementary

A graph $G$ has two proper subgraphs $G_1$ and $G_2$ such that $V(G) = V(G_1) = V(G_2)$, $E(G_1) \cap E(G_2) = \emptyset$, and $E(G_1) \cup E(G_2) = E(G)$. Thereby, we call $(G_1, G_2)$ a *G-matching*. Accordingly, we have the *G-complementary mixed graphic lattice* like that defined in Equation (28).

## 4. Encrypting Networks in Whole

In asymmetric topology cryptography, one would encrypt graphs (resp. networks) by mixed graphic groups, and we call these colorings *mixed graphic group colorings*. For the number $N_m$ of graphs of $n$ vertices, Harary and Palmer [26] computed two graph numbers

$$\begin{aligned} N_{23} &= 55994693969979208059797638081946217981227634845898163 2 \approx 2^{179} \\ N_{24} &= 19570490630207844792217486241672625600412207526706336575436 8 \approx 2^{197}. \end{aligned} \tag{29}$$

The large number of graphs, and of colorings in graph theory, can provide us with flexible and diverse asymmetric topology technology with stable security performance and can also increase the technical cost and intolerable time cost to the cracker. Encrypting networks in whole is an application of mixed graphic groups and mixed graphic group lattices.

### *4.1. Mixed Graphic Group Colorings in Encrypting Networks*

Here, we present a proof for the following theorem, as shown partly in Ref. [16]:

**Theorem 6.** *For each graph $L$ of a graphic $\boldsymbol{B}$-group lattice $\boldsymbol{L}(F_{m,n}[\ominus]\boldsymbol{B})$ defined in Definition 5, Equations (23) and (24) form an every-zero mixed graphic group $\{F_\alpha(L); [+]\}$ defined in Remark 1, where the graph $L$ admits a total coloring $\alpha$.*

**Proof.** Suppose that a $(p, q)$-graph $G$ admits a total coloring $f$ and $L$ is a graph of a graphic $\boldsymbol{B}$-group lattice $\boldsymbol{L}(F_{m,n}[\ominus_k]\boldsymbol{B})$, so $L = H[\ominus_k]_{j=1}^{M} a_j B_j$ as defined in Equation (23) and Definition 5.

Notice that each graph $G_{s,k} \in \boldsymbol{G}$ defined in Remark 1 admits a $W$-constraint proper total coloring $g_{s,k}$ in Definition 4. Suppose the graph $L$ admits a total coloring $\varphi : V(L) \cup$

$E(L) \to \boldsymbol{G}$, then each edge $uv \in E(L)$ holds $\varphi(uv) = G_{i_{uv},j_{uv}} \in \boldsymbol{G}$, $\varphi(u) = G_{i_u,j_u} \in \boldsymbol{G}$ and $\varphi(v) = G_{i_v,j_v} \in \boldsymbol{G}$, such that

$$G_{i_{uv},j_{uv}} = \varphi(uv) = \varphi(u)[+_{a,b}]\varphi(v) = G_{i_u,j_u}[+_{a,b}]G_{i_v,j_v} \tag{30}$$

with $i_{uv} = i_u + i_v - a \pmod p$ and $j_{uv} = j_u + j_v - b \pmod q$, under a preappointed zero $G_{a,b} \in \boldsymbol{G}$. In the graph $L$, there is at least one edge between $\varphi(u) = G_{i_u,j_u}$ and $\varphi(uv) = G_{i_{uv},j_{uv}}$, and there is at least one edge between $\varphi(v) = G_{i_v,j_v}$ and $\varphi(uv) = G_{i_{uv},j_{uv}}$.

Now, let us define a total coloring $\alpha$ for the graph $L$ as follows:

(i) $\alpha(w) = g_{s,k}(w)$ for each element $w \in V(G_{s,k}) \cup E(G_{s,k}) \subset V(L) \cup E(L)$ if $G_{s,k} \subset L$.

(ii) For an edge $xy \in E(L)$ holding $x \in V(G_{s,k})$ and $y \in V(G_{i,j})$, we color this edge $xy$ with $\alpha(xy) = g_{s,k}(x) + g_{i,j}(y) \pmod q$.

Next, we shall make the copies $L_{i,j}$ of the graph $L$ with $L_{i,j} \cong L$ for $i \in [1, p^*]$ and $j \in [1, q^*]$, where $p^* = |V(L)|$ and $q^* = |E(L)|$, and then put the copies into a set $S(L) = \{L_{i,j} : i \in [1, p^*], j \in [1, q^*]\}$. Moreover, we define a total coloring $\beta_{i,j}$ for each graph $L_{i,j}$ by setting

(i) $\beta_{i,j}(u) = \alpha(u) + i \pmod{p^*}$ for each vertex $u \in V(L_{i,j})$;

(ii) $\beta_{i,j}(uv) = \alpha(uv) + j \pmod{q^*}$ for each edge $uv \in E(L_{i,j})$;

(iii) For an edge $xy \in E(L)$ holding $x \in V(G_{s,k})$ and $y \in V(G_{i,j})$, we color this edge $xy$ with $\beta_{s,k}(x) + \beta_{i,j}(y) \pmod{q^*}$.

For a preappointed zero $L_{a,b} \in S(L)$, we have the following Abelian additive operation "$L_{i,j}[+_{a,b}]L_{s,k}$":

$$L_{i,j}[+_{a,b}]L_{s,k} := L_{i,j}[+]L_{s,k}[-]L_{a,b} = L_{\lambda,\mu} \in S(L) \tag{31}$$

for any two graphs $L_{i,j}, L_{s,k} \in S(L)$, such that

$$\beta_{i,j}(w) + \beta_{s,k}(w) - \beta_{a,b}(w) = \beta_{\lambda,\mu}(w) \tag{32}$$

holds true as $\lambda = i + s - a \pmod{p^*}$ and $\lambda = j + k - b \pmod{q^*}$.

We show that the set $S(L)$ holds the following facts:

(i) *Zero*. Every graph $L_{a,b} \in S(L)$ can be as *zero* such that $L_{i,j}[+_{a,b}]L_{a,b} := L_{i,j}$ for any graph $L_{i,j}$ of $S(L)$.

(ii) *Closure law*. For each preappointed zero $L_{a,b}$, we have

$$L_{i,j}[+_{a,b}]L_{s,k} := L_{i,j}[+]L_{s,k}[-]L_{a,b} = L_{\lambda,\mu} \in S(L)$$

(iii) *Inverse*. Every graph $L_{i,j} \in S(L)$ has its own *inverse* $L_{i^{-1},j^{-1}} \in S(L)$ with $i^{-1} = 2a - i$ and $j^{-1} = 2b - j$, such that $L_{i,j}[+_{a,b}]L_{i^{-1},j^{-1}} := L_{a,b}$.

(iv) *Associative law*. $\big(L_{i,j}[+_{a,b}]L_{s,k}\big)[+_{a,b}]L_{c,d} = L_{i,j}[+_{a,b}]\big(L_{s,k}[+_{a,b}]L_{c,d}\big)$.

(v) *Commutative law*. $L_{i,j}[+_{a,b}]L_{s,k} = L_{s,k}[+_{a,b}]L_{i,j}$.

Thereby, the set $S(L)$ forms an every-zero mixed graphic group, denoted as $S(L) = \{F_\alpha(L); [+]\}$, and the set $S(L)$ is a *graphic category* under the graphic morphism composition defined in Equation (16).

We can define another total coloring $\gamma_{i,j}$ for each graph $L_{i,j} \in S(L)$ by making

(i) $\gamma_{i,j}(x) = \alpha(x) + i \pmod p$ for each vertex $x \in V(L_{i,j})$;

(ii) $\gamma_{i,j}(xy) = \alpha(xy) + j \pmod q$ for each edge $xy \in E(L_{i,j})$;

(iii) For an edge $uv \in E(L)$ holding $x \in V(G_{s,k})$ and $y \in V(G_{i,j})$, we color this edge $uv$ with $\gamma_{s,k}(u) + \gamma_{i,j}(v) \pmod q$, such that the set $S(L)$ forms an every-zero mixed graphic group $S(L) = \{F_\alpha(L); [+]\}$.

The proof of the theorem is complete. □

*4.2. Encrypting Tree-like Networks*

As tree-like networks are easily accessible in real applications, have simple structures, and admit a lot of colorings, we will apply *mixed graphic group colorings* to encrypt tree-like networks. A tree $T$ admits a mixed graphic group total coloring

$$\theta : V(T) \cup E(T) \to \boldsymbol{G} = \{M_f(G); [+]\}$$

as defined in Remark 1, where $M_f(G) = \{G_{i,j} : i \in [1,p], j \in [1,q]\}$.

**Theorem 7.** *A tree $T$ with its maximum degree $\Delta$ admits a* mixed graphic group total coloring $\theta$ *from $V(T) \cup E(T)$ to a mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1 and $pq > \Delta$, such that $\theta(uv) \neq \theta(uw)$ for any pair of adjacent edges $uv$ and $uw$ of $T$.*

**Proof.** We construct another tree $H = T - wz$ by removing a leaf $w$ of the tree $T$, where the leaf $w$ is adjacent to the vertex $z$ of $T$, and keep the maximum degree $\Delta(H) = \Delta(T)$. Assume that the tree $H = T - wz$ admits a mixed graphic group total coloring $h$ from $V(H) \cup E(H)$ to a mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1 and $pq > \Delta(H)$, such that the colors $h(uv) \neq h(uw)$ for any pair of adjacent edges $uv$ and $uw$ of $H$.

Let $N(z) = \{x_1, x_2, \ldots, x_k, w\}$ be the set of neighboring vertices of the vertex $z$ in the tree $T$. We define a mixed graphic group total coloring $\theta : V(T) \cup E(T) \to \boldsymbol{G} = \{M_f(G); [+]\}$ as $\theta(x) = h(x)$ for $x \in V(T) \cup E(T) \setminus \{w, wz\}$, $\theta(wz) = G_{i_0,j_0} \in \boldsymbol{G} \setminus \{h(zx_i) : i \in [1,k]\}$, and $\theta(w) = G_{s_0,k_0} \in \boldsymbol{G} \setminus \{h(z), h(zx_i) : i \in [1,k]\}$, such that $\theta(wz) = h(z)[+_{a,b}]\theta(w)$ under a preappointed zero $G_{a,b} \in \boldsymbol{G}$.

We obtain the proof of the theorem. □

**Theorem 8.** *Each tree $T$ of $n$ edges admits a* mixed graphic group total coloring $\theta$ *from $V(T) \cup E(T)$ to a mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1, such that the edge index set $\{(i,j) : \theta(u_iv_j) = G_{i,j} \in \boldsymbol{G},\ u_iv_j \in E(T)\} = X$, where $X = \{(i_1,j_1), (i_2,j_2), \ldots, (i_n,j_n)\}$ with $(i_s,j_s) \neq (i_k,j_k)$ for $s \neq k$ is a preappointed index set.*

**Proof.** Assume that any tree $T$ of $n-1$ edges holds this theorem and $T$ admits a mixed graphic group total coloring $F : V(T) \cup E(T) \to \boldsymbol{G}$, such that each edge $uv \in E(T)$ is colored with

$$G_{\lambda,\mu} = F(uv) = F(u)[+_{a,b}]F(v) = G_{i,j}[+_{a,b}]G_{s,k}$$

under a preappointed zero $G_{a,b} \in \boldsymbol{G}$, and the edge index set is just

$$\{(\lambda,\mu) : F(u_\lambda v_\mu) = G_{\lambda,\mu} \in \boldsymbol{G},\ u_\lambda v_\mu \in E(T)\} = X \setminus \{(i_n,j_n)\}.$$

We add a new vertex $w$ to the tree $T$ by joining $w$ with any vertex $x$ of $T$ via a new edge $xw$. The resulting tree is denoted as $H = T + \{w, xw\}$. Obviously, the tree $H$ has $n$ vertices.

We define a mixed graphic group total coloring $\theta : V(H) \cup E(H) \to \boldsymbol{G}$, such that each element $z \in V(T) \cup E(T) \subset V(H) \cup E(H)$ is colored with $\theta(z) = F(z)$.

For the vertex $w$ and the edge $xw$ of the tree $H = T + \{w, xw\}$, we set $\theta(w) = G_{\alpha,\beta}$ and $\theta(xw) = G_{i_n,j_n} \in \boldsymbol{G} \setminus \theta(E(T))$ such that

$$G_{i_n,j_n} = \theta(xw) = \theta(x)[+_{a,b}]\theta(w) = G_{\gamma,\delta}[+_{a,b}]G_{\alpha,\beta}$$

with $i_n = \gamma + \alpha - a \pmod p$ and $j_n = \delta + \beta - b \pmod q$, where the edge color set $\theta(E(T)) = \{G_{\lambda,\mu} : F(uv) = G_{\lambda,\mu} \in \boldsymbol{G},\ uv \in E(T)\}$. Finally, we obtain the desired edge index set

$$\{(i,j) : \theta(x_iy_j) = G_{i,j} \in \boldsymbol{G},\ x_iy_j \in E(H)\} = X$$

and the theorem follows from the induction. □

**Corollary 1.** *If a connected graph $H$ of $n$ edges admits a* mixed graphic group total coloring *$\theta$ from $V(H) \cup E(H)$ to a mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1, such that the edge index set $I_{ndex} = \{(i,j) : \theta(u_iv_j) = G_{i,j} \in \boldsymbol{G},\ u_iv_j \in E(H)\}$, where $I_{ndex} = \{(i_1,j_1),(i_2,j_2),\ldots,(i_n,j_n)\}$ with $(i_s,j_s) \neq (i_k,j_k)$ for $s \neq k$ is a preappointed edge index set, then the connected graph $H$ corresponds to at least a tree $T$ of $n$ edges such that $T$ holds Theorem 8, and there is a* colored graph homomorphism *$T \to_{color} H$.*

**Theorem 9.** *The edges of a tree $T$ can be colored arbitrarily by a mixed graphic group proper edge coloring $\varphi$ from the edge set $E(T)$ to a mixed graphic group $\boldsymbol{G} = \{M_f(G); [+]\}$ defined in Remark 1, and then this mixed graphic group proper edge coloring $\varphi$ can be expended to the vertex set $V(T)$, such that each edge $uv \in E(T)$ holds $\varphi(uv) = \varphi(u)[+_{a,b}]\varphi(v)$ under a preappointed zero $G_{a,b} \in \boldsymbol{G}$.*

**Proof.** Let $G_{a,b} \in \boldsymbol{G}$ be a preappointed zero. Suppose that a tree $T$ of $p$ vertices admits a mixed graphic group edge coloring $F : E(T) \to \boldsymbol{G}$, and this coloring $F$ has been expended to $V(T)$, such that $F(uv) = F(u)[+_{a,b}]F(v)$ for each edge $uv \in E(T)$, and $F(uv) \neq F(uw)$ for any pair of adjacent edges $uv, uw \in E(T)$. We construct a new tree $H = T + \{w, xw\}$ by adding a new vertex $w$ to the tree $T$ and a new edge $xw$ with $x \in E(T)$.

For this new tree $H$, we define a mixed graphic group edge coloring $\varphi : E(H) \to \boldsymbol{G}$ with $\varphi(uv) = F(uv)$ if $uv \in E(T) \subset E(H)$, and the mixed graphic group edge coloring $\varphi$ can be expended to $V(T) \subset V(H)$, such that $\varphi(uv) = \varphi(u)[+_{a,b}]\varphi(v)$ for each edge $uv \in E(T)$ by the induction. Next, we take $\varphi(w) = G_\alpha \in \boldsymbol{G}$ and $\varphi(xw) = G_\lambda \in \boldsymbol{G} \setminus \{\varphi(xy_i) : y_i \in N(x)\}$ holding $G_\lambda = \varphi(xw) = \varphi(x)[+_{a,b}]\varphi(w) = G_\beta[+_{a,b}]G_\alpha$ with $\lambda = \alpha + \beta - k \pmod q$. Finally, we expend the mixed graphic group proper edge coloring $\varphi$ to $V(H)$, such that $\varphi(xy) = \varphi(x)[+_{a,b}]\varphi(y)$ for each edge $xy \in E(H)$, and $\varphi(uv) \neq \varphi(uw)$ for any pair of adjacent edges $uv, uw \in E(H)$; thus, the induction is complete. □

### *4.3. Graphic Lattices for the Encryption of Dynamic Networks*

For the encryption of dynamic networks, we define the following every-zero dynamically mixed graphic group: an every-zero dynamically mixed graphic group $\boldsymbol{G}(t) = \{M_{f_t}(G); [+]\}$ is based on a dynamically colored graph set $M_{f_t}(G) = \{G_{i,j}(t) : i \in [1,p], j \in [1,q]\}$ with $G_{s,k}(t) \cong G(t)$ for $t \in [\alpha,\beta]$, where a $(p,q)$-graph $G(t)$ admits a $W$-constraint proper total coloring $f_t : V(G) \cup E(G) \to [1,n(t)]$ for $t \in [\alpha,\beta]$, and each graph $G_{i,j}(t)$ admits a $W$-constraint proper total coloring $g^t_{s,k}(x) = f_t(x) + s \pmod p$ for every vertex $x \in V(G_{i,j}(t))$, and $g^t_{s,k}(uv) = f_t(uv) + k \pmod q$ for each edge $uv \in E(G_{i,j}(t))$.

Obviously, $\boldsymbol{G}(t) = \{M_{f_t}(G); [+]\}$ for $t \in [\alpha,\beta]$ forms *dynamically graphic categories*.

With the dynamically colored graph set $M_{f_t}(G) = \{G_{i,j}(t) : i \in [1,p], j \in [1,q]\}$, we have a *dynamically mixed graphic lattice base* as follows:

$$\begin{aligned}\boldsymbol{B}(t) &= (G_{1,1}(t), G_{2,1}(t), \ldots, G_{p,1}(t), \ldots, G_{s,k}(t), \ldots, G_{p,1}(t), G_{p,2}(t), \ldots, G_{p,q}(t)) \\ &= (B_1(t), B_2(t), \ldots, B_M(t)),\end{aligned} \tag{33}$$

where $M = pq$. For a graph operation "$(\bullet)$", we have a *dynamically mixed graphic lattice*

$$\boldsymbol{L}(F_{m,n}(t)(\bullet)\boldsymbol{B}(t)) = \left\{H(t)(\bullet)_{k=1}^{M} a_k B_k(t) : a_k \in Z^0,\ B_k(t) \in \boldsymbol{B}(t),\ H(t) \in F_{m,n}(t)\right\} \tag{34}$$

such that each network $H(t)$ is encrypted to another graph $L(t) = H_t(\bullet)_{k=1}^{M} a_k B_k(t)$ for $t \in [\alpha,\beta]$, where $\sum_{k=1}^{M} a_k \geq 1$.

As the graph operation "$(\bullet)$" in Equation (34) is the vertex-coinciding operation, an example is shown in Figure 8.

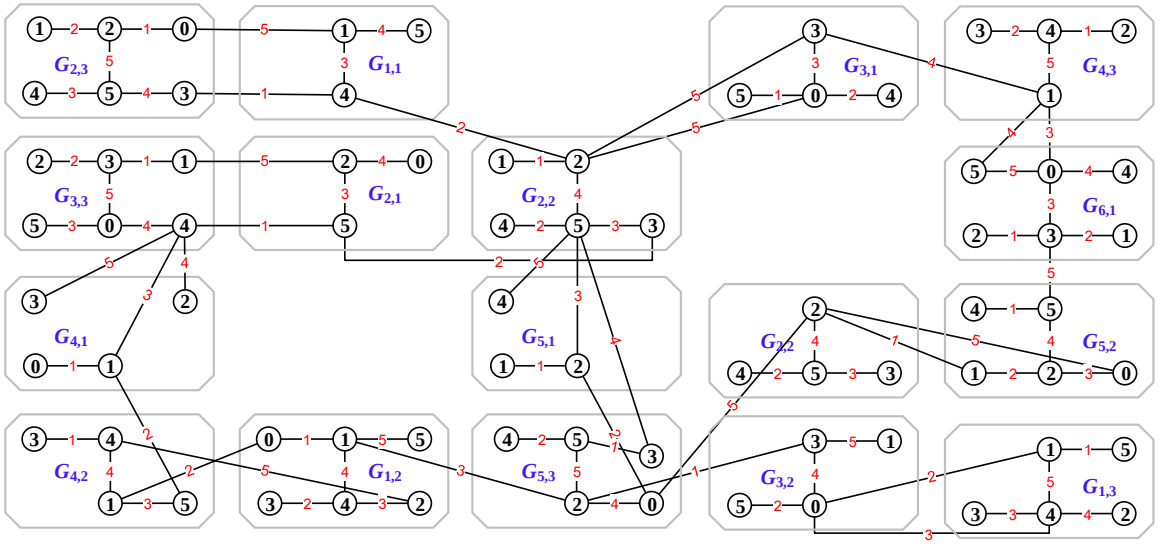



**Figure 8.** A graph $Q$ for illustrating the vertex-coinciding operation in the dynamically mixed graphic lattice shown in Equation (34) based on the every-zero mixed graphic group $M_f(G) = \{G_{s,k} : s \in [1,6], k \in [1,5]\}$ shown in Figure 1.

## 5. Summary

To summarize, in the present contribution we firstly defined the graphic category, generalized the mixed graphic groups, and proposed the graphic lattices and various graph-type homomorphisms, from which some useful results were obtained. Based on these results, we then discussed in detail how to encrypt networks in whole by using the mixed graphic groups and the mixed graphic group lattices. In the end, the graphic lattices for the encryption of the dynamic networks were introduced, and the vertex-coinciding operation in the dynamically mixed graphic lattice was illustrated on the basis of the every-zero mixed graphic groups.

**Author Contributions:** Conceptualization, M.Z. and B.Y.; methodology, M.Z. and B.Y.; investigation, M.Z. and B.Y.; writing—original draft, M.Z.; and writing—review & editing, H.W. and B.Y. All authors have read and agreed to the published version of the manuscript.

**Funding:** The Science and Technology Program of Gansu Province under Grant No. 22JR5RA876 and the National Natural Science Foundation of China under Grants No. 61163054, No. 61363060, and No. 61662066.

**Institutional Review Board Statement:** Not applicable.

**Data Availability Statement:** The data used to support the findings of this study are included within the article.

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

## References

1. Wang, X.; Liu, M. Survey of lattice-based cryptography. *J. Cryptologic Res.* **2014**, *1*, 13–27. (In Chinese)
2. Anshel, I.; Anshel, M.; Goldfeld, D. An algebraic method for public-key cryptography. *Math. Res. Lett.* **1999**, *6*, 287–291. [CrossRef]
3. Eick, B.; Kahrobaei, D. A new platform for cryptology? *arXiv* **2004**, arXiv:math/0411077v1.
4. Ostrovsky, R.; Skeith, W.E., III. Communication complexity in algebraic two-party protocols. In Proceedings of the 28th Annual International Cryptology Conference (Advances in Cryptology—CRYPTO 2008), Santa Barbara, CA, USA, 17–21 August 2008; pp. 379–396.
5. Flores, R.; Kahrobaei, D.; Koberda, T. Algorithmic problems in right-angled Artin groups: Complexity and applications. *J. Algebra* **2019**, *519*, 111–129. [CrossRef]
6. Kahrobaei, D.; Tortora, A.; Tota, M. Multilinear cryptography using nilpotent groups. *arXiv* **2019**, arXiv:1902.08777v2.
7. Anshel, I.; Atkins, D.; Goldfeld, D.; Gunnells, P.E. WalnutDSA™: A group theoretic digital signature algorithm. *Int. J. Comput. Math. Comput. Syst. Theory* **2021**, *6*, 260–284. [CrossRef]

8. Kahrobaei, D.; Flores, R.; Noce, M. Group-based cryptography in the quantum era. *Not. Am. Math. Soc.* **2023**, *70*, 2–13. [CrossRef]
9. Yao, B.; Sun, H.; Zhao, M.; Li, J.; Yan, G. On coloring/labelling graphical groups for creating new graphical passwords. In Proceedings of the 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC 2017), Chengdu, China, 15–17 December 2017; pp. 1371–1375.
10. Sun, H.; Zhang, X.; Zhao, M.; Yao, B. New algebraic groups produced by graphical passwords based on colorings and labellings. In Proceedings of the MATEC Web Conference (ICMITE 2017), Chengdu, China, 16–17 December 2017; Volume 139, p. 00152.
11. Yao, B.; Mu, Y.; Sun, H.; Zhang, X.; Wang, H.; Su, J.; Ma, F. Algebraic groups for construction of topological graphic passwords in cryptography. In Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC 2018), Chongqing, China, 12–14 October 2018; pp. 2211–2216.
12. Yao, B.; Sun, H.; Su, J.; Wang, H.; Zhao, M. Various matchings of graphic groups for graphic lattices in topological coding. In Proceedings of the ICIBA 2020, Chongqing China, 6–8 November 2020; pp. 1–6.
13. Zhao, M.; Yao, M.; Zhang, X.; Sun, Y.; Yao, B. Coding graphic groups for network security. In Proceedings of the IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC 2019), Chengdu, China, 20–22 December 2019; pp. 2118–2122.
14. Zhao, M.; Yao, M.; Yao, B. On modular-2q graphic groups of topological coding for graphic passwords. In Proceedings of the IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 6–8 November 2020; pp. 458–462.
15. Wang, H.; Su, J.; Yao, B. Graphic groups towards cryptographic systems resisting classical and quantum computers. In Proceedings of the IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 12–14 June 2020.
16. Yao, B. Graphic lattices and matrix lattices of topological coding. *arXiv* **2020**, arXiv:2005.03937v1.
17. Bondy, J.A.; Murty, U.S.R. *Graph Theory*; Springer: London, UK, 2008.
18. Bondy, J.A.; Murty, U.S.R. *Graph Theory with Application*; MacMillan: London, UK, 1976.
19. Bang-Jensen, J.; Gutin, G. *Digraphs: Theory, Algorithms and Applications*; Springer: Berlin/Heidelberg, Germany, 2007.
20. Gallian, J.A. A dynamic survey of graph labeling. *Electron. J. Comb.* **2022** . [CrossRef] [PubMed]
21. Yao, B.; Wang, H. Recent colorings and labelings in topological coding. *arXiv* **2021**, arXiv:2106.15254v1.
22. Yao, B.; Zhang, X.; Sun, H.; Su, J.; Ma, F.; Wang, H. Parameterized colorings and labellings of graphs in topological coding. *arXiv* **2022**, arXiv:2207.03381v1.
23. Yao, B.; Sun, H.; Zhang, X.; Mu, Y.; Sun, Y.; Wang, H.; Su, J.; Zhang, M.; Yang, S.; Yang, C. Topological graphic passwords and their matchings towards cryptography. *arXiv* **2018**, arXiv:1808.03324v1.
24. Wang, H.; Xu, J.; Yao, B. Twin odd-graceful trees towards information security. *Procedia Comput. Sci.* **2017**, *107*, 15–20. [CrossRef]
25. Yao, B.; Liu, X.; Yao, M. Connections between labellings of trees. *Bull. Iran. Math. Soc.* **2017**, *43*, 275–283.
26. Harary, F.; Palmer, E.M. *Graphical Enumeration*; Academic Press: Cambridge, MA, USA, 1973.