entropy

MDPI

Article

Reduction Theorem for Secrecy over Linear Network Code for Active Attacks †

Masahito Hayashi [1,2,3,4,*,‡], Masaki Owari [5], Go Kato [6] and Ning Cai [7,‡]

1 Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
2 Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
3 Shenzhen Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
4 Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan
5 Department of Computer Science, Faculty of Informatics, Shizuoka University, Shizuoka 422-8529, Japan; masakiowari@inf.shizuoka.ac.jp
6 NTT Communication Science Laboratories, NTT Corporation, Tokyo 100-8116, Japan; go.kato.gm@hco.ntt.co.jp
7 The School of Information Science and Technology, ShanghaiTech University, Middle Huaxia Road no. 393, Pudong, Shanghai 201210, China; ningcai@shanghaitech.edu.cn
* Correspondence: hayashi@sustech.edu.cn
† Parts of this paper were presented at the 2017 IEEE International Symposium on Information Theory (ISIT 2017), Aachen, Germany, 25–30 June 2017.
‡ These authors contributed equally to this work.

Received: 27 August 2020; Accepted: 16 September 2020; Published: 21 September 2020

Abstract: We discuss the effect of sequential error injection on information leakage under a network code. We formulate a network code for the single transmission setting and the multiple transmission setting. Under this formulation, we show that the eavesdropper cannot increase the power of eavesdropping by sequential error injection when the operations in the network are linear operations. We demonstrated the usefulness of this reduction theorem by applying a concrete example of network.

Keywords: secrecy analysis; secure network coding; sequential injection; passive attack; active attack

1. Introduction

Secure network coding offers a method for securely transmitting information from an authorized sender to an authorized receiver. Cai and Yeung [1] discussed the secrecy of when a malicious adversary, Eve, wiretaps a subset E_E of the set E of all the channels in a network. Using the universal hashing lemma [2–4], the papers [5,6] showed the existence of a secrecy code that works universally for any type of eavesdropper when the cardinality of E_E is bounded. In addition, the paper [7] discussed the construction of such a code. As another type of attack on information transmission via a network, a malicious adversary contaminates the communication by changing the information on a subset E_A of E. Using an error correcting code, the papers [8–11] proposed a method to protect the message from contamination. That is, we require that the authorized receiver correctly recovers the message, which is called robustness.

As another possibility, we consider the case when the malicious adversary combines eavesdropping and contamination. That is, by contaminating a part of the channels in the network, the malicious adversary might increase the ability of eavesdropping, whereas a parallel network offers no such a possibility [12–14]. In fact, in arbitrarily varying channel model, noise injection is allowed

after Eve's eavesdropping, but Eve does not eavesdrop the channel after Eve's noise injection [15–19]. The paper [20] also discusses secrecy in the same setting while it addresses the network model. The studies [7,14] discussed the secrecy when Eve eavesdrops the information transmitted on the channels in E_E after noises are injected in E_A, but they assume that Eve does not know the information of the injected noise.

In contrast, this paper focuses on a network, and discusses the secrecy when Eve adds artificial information to the information transmitted on the channels in E_A, eavesdrops on the information transmitted on the channels in E_E, and estimates the original message from the eavesdropped information and the information of the injected noises. We call this type of attack an active attack and call an attack without contamination a passive attack. We call each of Eve's active operations a strategy. When $E_A \subset E_E$ and any active attack are available for Eve, she is allowed to arbitrarily modify the information on the channels in E_A sequentially based on the obtained information.

This paper aims to show a reduction theorem for an active attack, i.e., the fact that no strategy can increase Eve's information when every operation in the network is linear and Eve's contamination satisfies a natural causal condition. When the network is not well synchronized, Eve can make an attack across several channels. This reduction theorem holds even under this kind of attack. In fact, there is an example having a non-linear node operation such that Eve can increase her performance to extract information from eavesdropping an edge outgoing an intermediate node by adding artificial information to an edge incoming the intermediate node [21] (The paper [21] also discusses linear code; it discusses only code a on one-hop relay network. Our results can be applied to general networks.) This example shows the necessity of linearity for this reduction theorem. Although our discussion can be extended to the multicast and multiple-unicast cases, for simplicity, we consider the unicast setting in the following discussion.

Further, we apply our general result to the analysis of a concrete example of a network. In this network, we demonstrate that any active attack cannot increase the performance of eavesdropping. However, in the single transmission case over the finite field $\mathbb{F}_2$, the error correction and the error detection are impossible over this contamination. To resolve this problem, this paper addresses the multiple transmission case in addition to the single transmission case. In the multiple transmission case, the sender uses the same network multiple times, and the topology and dynamics of the network do not change during these transmissions. While several papers discussed this model, many of them discussed the multiple transmission case only with contamination [22–24] or eavesdropping [5,6,25–27]. Only the paper [20] addressed it with contamination and eavesdropping, and its distinction from the paper [20] is summarized as follows. The paper [20] assumes that all injections are done after eavesdropping, while this paper allows Eve to inject the artificial information before a part of eavesdropping.

We formulate the multiple transmission case when each transmission has no correlation with the previous transmission while injected noise might have such a correlation. Then, we show the above type of reduction theorem for an active attack even under the multiple transmission case. We apply this result to the multiple transmission over the above example of a network, in which the error correction and the error detection are possible over this contamination. Hence, the secrecy and the correctness hold in this case.

The remaining part of this paper is organized as follows. Section 2 discusses the single transmission setting that has only a single transmission, and Section 3 discusses the multiple transmission setting that has n transmissions. Two types of multiple transmission setting are formulated. Then, we state our reduction theorem in both settings. In Section 4, we state the conclusion.

2. Single Transmission Setting

2.1. Generic Model

In this subsection, we give a generic model, and discuss its relation with a concrete network model in the latter subsections. We consider the unicast setting of network coding on a network.

Assume that the authorized sender, Alice, intends to send information to the authorized receiver, Bob, via the network. Although the network is composed of m_1 edges and m_2 vertecies, as shown later, the model can be simplified as follows when the node operations are linear. We assume that Alice inputs the input variable $\mathbf{X}$ in $\mathbb{F}_q^{m_3}$ and Bob receives the output variable $\mathbf{Y}_B$ in $\mathbb{F}_q^{m_4}$, where $\mathbb{F}_q$ is a finite field whose order is a power q of a prime p. We also assume that the malicious adversary, Eve, wiretaps the information $\mathbf{Y}_E$ in $\mathbb{F}_q^{m_6}$ This network has $m_7 = m_1 - m_3$ edges that are not directly linked to the source node. The parameters are summarized as Table 1. (In this paper, we denote the vector on $\mathbb{F}_q$ by a bold letter, but we use a non-bold letter to describe a scalar and a matrix).

Table 1. Channel parameters.

m_1	Number of edges
m_2	Number of vertecies
m_3	Dimension of Alice's input information $\mathbf{X}$
m_4	Dimension of Bob's observed information $\mathbf{Y}_B$
m_5	Dimension of Eve's injected information $\mathbf{Z}$
m_6	Dimension of Eve's wiretapped information $\mathbf{Y}_E$
m_7	$m_1 - m_3$

Then, we adopt the model with matrices $K_B = [K_{B;j,i}] \in \mathbb{F}_q^{m_4 \times m_3}$ and $K_E = [K_{E;j,i}] \in \mathbb{F}_q^{m_6 \times m_3}$, in which the variables $\mathbf{X}$, $\mathbf{Y}_B$, and $\mathbf{Y}_E$ satisfy their relations

$$\mathbf{Y}_B = K_B\mathbf{X}, \quad \mathbf{Y}_E = K_E\mathbf{X}. \tag{1}$$

This attack is a conventional wiretap model and is called a passive attack to distinguish it from an active attack, which will be introduced later. Section 2.3 will explain how this model is derived from a directed graph with E_E and linear operations on nodes.

In this paper, we address a stronger attack, in which Eve injects noise $\mathbf{Z} \in \mathbb{F}_q^{m_5}$. Hence, using matrices $H_B = [H_{B;j,i}] \in \mathbb{F}_q^{m_4 \times m_5}$ and $H_E = [H_{E;j,i}] \in \mathbb{F}_q^{m_6 \times m_5}$, we rewrite the relations (1) as

$$\mathbf{Y}_B = K_B\mathbf{X} + H_B\mathbf{Z}, \quad \mathbf{Y}_E = K_E\mathbf{X} + H_E\mathbf{Z}, \tag{2}$$

which is called a wiretap and addition model. The i-th injected noise Z_i (the i-th component of $\mathbf{Z}$) is decided by a function α_i of $\mathbf{Y}_E$. Although a part of $\mathbf{Y}_E$ is a function of α_i, this point does not make a problem for causality, as explained in Section 2.5. In this paper, when a vector has the j-th component x_j; the vector is written as $[x_j]_{1 \le j \le a}$, where the subscript $1 \le j \le a$ expresses the range of the index j. Thus, the set $\alpha = [\alpha_i]_{1 \le i \le m_5}$ of the functions can be regarded as Eve's strategy, and we call this attack an active attack with a strategy α. That is, an active attack is identified by a pair of a strategy α and a wiretap, and an addition model decided by $\boldsymbol{K}, \boldsymbol{H}$. Here, we treat K_B, K_E, H_B, and H_E as deterministic values, and denote the pairs (K_B, K_E) and (H_B, H_E) by $\boldsymbol{K}$ and $\boldsymbol{H}$, respectively. Hence, our model is written as the triplet $(\boldsymbol{K}, \boldsymbol{H}, \alpha)$. As shown in the latter subsections, under the linearity assumption on the node operations, the triplet $(\boldsymbol{K}, \boldsymbol{H}, \alpha)$ is decided from the network topology (a directed graph with E_A and E_E) and dynamics of the network. Here, we should remark that the relation (2) is based on the linearity assumption for node operations. Since this assumption is the restriction for the protocol, it does not restrict the eavesdropper's strategy.

We impose several types for regularity conditions for Eve's strategy α, which are demanded from causality. Notice that α_i is a function of the vector $[Y_{E,j}]_{1 \le j \le m_6}$. Now, we take the causality with respect to α into account. Here, we assume that the assigned index i for $1 \le i \le m_5$ expresses the time-ordering of injection. That is, we assign the index i for $1 \le i \le m_5$ according to the order of injections. Hence, we assume that α_i is decided by a part of Eve's observed variables. We say that

subsets $w_i \subset \{1, \ldots, m_6\}$ for $i \in \{1, \ldots, m_5\}$ are the domain index subsets for α when the function α_i is given as a function of the vector $[Y_{E,j}]_{j \in w_i}$. Here, the notation $j \in w_i$ means that the j-th eavesdropping is done before the i-th injection; i.e., w_i expresses the set of indexes corresponding to the symbols that do effect the i-th injection. Hence, the eavesdropped symbol $Y_{E,j}$ does not depend on the injected symbol z_i for $j \in w_i$. Since the decision of the injected noise does not depend on the consequences of the decision, we introduce the following causal condition.

Definition 1. *We say that the domain index subsets $\{w_i\}_{1,\ldots,m_5}$ satisfy the causal condition when the following two conditions hold:*

(A1) *The relation $H_{E;j,i} = 0$ holds for $j \in w_i$.*
(A2) *The relation $w_1 \subseteq w_2 \subseteq \ldots \subseteq w_{m_5}$ holds.*

As a necessary condition of the causal condition, we introduce the following uniqueness condition for the function α_i, which is given as a function of the vector $[Y_{E,j}]_{1 \le j \le m_6}$.

Definition 2. *For any value of $\mathbf{x}$, there uniquely exists $\mathbf{y} \in \mathbb{F}_q^{m_6}$ such that*

$$\mathbf{y} = K_E \mathbf{x} + H_E \alpha(\mathbf{y}). \tag{3}$$

This condition is called the uniqueness condition for α.

When the uniqueness condition does not hold, for an input $\mathbf{x}$, there exist two vectors $\mathbf{y}$ and $\mathbf{y}'$ to satisfy (3). It means that both outputs $\mathbf{y}$ and $\mathbf{y}'$ may happen; nevertheless, all the operations are deterministic. This situation is unlikely in a real word. Examples of a network with w_i, $[H_{E;j,i}]_{i,j}$ will be given in Section 2.6. Then, we have the following lemma, which shows that the uniqueness condition always holds under a realistic situation.

Lemma 1. *When a strategy α has domain index subsets to satisfy the causal condition, the strategy α satisfies the uniqueness condition.*

Proof. When the causal condition holds, we show the fact that $y_{j'}$ is given as a function of $K_E \mathbf{x}$ for any $j' \in w_i$ by induction with respect to the index $i = 1, \ldots, m_5$, which expresses the order of the injected information. This fact yields the uniqueness condition.

For $j \in w_1$, we have $y_j = (K_E \mathbf{x})_j$ because $(H_E \alpha(\mathbf{y}))_j$ is zero. Hence, the statement with $i = 1$ holds. We choose $j \in w_{i+1} \setminus w_i$. Let $z_{i'}$ be the i'-th injected information. Due to conditions (A1) and (A2), $y_j - (K_E \mathbf{x})_j = (H_E \mathbf{z})_j$ is a function of $z_1 = \alpha(\mathbf{y})_1, \cdots, z_i = \alpha(\mathbf{y})_i$. Since the assumption of the induction guarantees that $z_1, \ldots, z_i$ are functions of $[y_{j'}]_{j' \in w_i}$, $z_1, \ldots, z_i$ are functions of $K_E \mathbf{x}$. Then, we find that $y_j = (K_E \mathbf{x})_j + (H_E \mathbf{z})_j$ is given as a function of $K_E \mathbf{x}$ for any $j \in w_{i+1} \setminus w_i$. That is, the strategy α satisfies the uniqueness condition. □

Now, we have the following reduction theorem.

Theorem 1 (Reduction theorem)**.** *When the strategy α satisfies the uniqueness condition, Eve's information $\mathbf{Y}_E(\alpha)$ with strategy α can be calculated from Eve's information $\mathbf{Y}_E(0)$ with strategy 0 (the passive attack), and $\mathbf{Y}_E(0)$ is also calculated from $\mathbf{Y}_E(\alpha)$. Hence, we have the equation*

$$I(\mathbf{X}; \mathbf{Y}_E)[0] = I(\mathbf{X}; \mathbf{Y}_E)[\alpha], \tag{4}$$

$I(\mathbf{X}; \mathbf{Y}_E)[\alpha]$ expresses the mutual information between $\mathbf{X}$ and $\mathbf{Y}_E$ under the strategy α.

Proof. This proof can be done by showing that Eve's information with a strategy α can be simulated by Eve's information with a strategy 0 as follows.

Since $\mathbf{Y}_E(0) = K_E\mathbf{X}$ and $\mathbf{Y}_E(\alpha) = K_E\mathbf{X} + H_E\mathbf{Z}$, due to the uniqueness condition of the strategy α, we can uniquely evaluate $\mathbf{Y}_E(\alpha)$ from $\mathbf{Y}_E(0) = K_E\mathbf{X}$ and α. Therefore, we have $I(\mathbf{X};\mathbf{Y}_E)[0] \geq I(\mathbf{X};\mathbf{Y}_E)[\alpha]$. Conversely, since $\mathbf{Y}_E(0)$ is given as a function $(\mathbf{Y}_E(\alpha) - H_E\mathbf{Z})$ of $\mathbf{Y}_E(\alpha)$, $\mathbf{Z}$, and H_E, we have the opposite inequality. □

This theorem shows that the information leakage of the active attack with the strategy α is the same as the information leakage of the passive attack. Hence, to guarantee the secrecy under an arbitrary active attack, it is sufficient to show secrecy under the passive attack. However, there is an example of non-linear network such that this kind of reduction does not hold [21]. In fact, even when the network does not have synchronization so that the information transmission on an edges starts before the end of the information transmission on the previous edge, the above reduction theorem hold under the uniqueness condition.

2.2. Recovery and Information Leakage with Linear Code

Next, we consider the recovery and the information leakage when a linear code is used. Assume that a message $\mathbf{M} \in \mathbb{F}_q^\ell$ is generated subject to the uniform distribution and is sent via an encoding map, i.e., a linear map f_1 from $\mathbb{F}_q^\ell$ to $\mathbb{F}_q^{m_3}$. Additionally, Alice independently generates a scramble variable $\mathbf{L} \in \mathbb{F}_q^k$ subject to the uniform distribution and send it via another a linear map f_2 from $\mathbb{F}_q^k$ to $\mathbb{F}_q^{m_3}$. In this case, Alice transmits $f_1(\mathbf{M}) + f_2(\mathbf{L}) \in \mathbb{F}_q^{m_3}$, as is implicitly stated in many papers ([22] Section V; [23] Section V; [20] Section IV).

Proposition 1. *Bob is assumed to know the forms of K_B, H_B and f_1, f_2. Bob can correctly recover the message $\mathbf{M}$ with probability 1 if and only if* $\dim \operatorname{Im} K_B \circ f_1 = \ell$ *and* $\dim(\operatorname{Im} K_B \circ f_1 \cap (\operatorname{Im} K_B \circ f_2 + \operatorname{Im} H_B)) = 0$.

Proof. To recover the message M, the dimension $\dim \operatorname{Im} K_B \circ f_1$ needs to be ℓ. When $\dim(\operatorname{Im} K_B \circ f_1 \cap (\operatorname{Im} K_B \circ f_2 + \operatorname{Im} H_B)) > 0$, there exist vectors $\mathbf{m}_0 (\neq 0) \in \mathbb{F}_q^\ell$, $\mathbf{l}_0 \in \mathbb{F}_q^k$, and $\mathbf{z_0} \in \mathbb{F}_q^{m_5}$ such that $K_B(f_1(\mathbf{m}_0) + f_2(\mathbf{l}_0)) + H_B(\mathbf{z_0}) = 0$. Thus, Bob may receive 0 when the message $\mathbf{M}$ is 0 or $\mathbf{m}_0$. This fact means the impossibility of Bob's perfect recovery.

When $\dim \operatorname{Im} K_B \circ f_1 = \ell$ and $\dim(\operatorname{Im} K_B \circ f_1 \cap (\operatorname{Im} K_B \circ f_2 + \operatorname{Im} H_B)) = 0$, there exists a linear map P from $\mathbb{F}_q^{m_4}$ to $\operatorname{Im} K_B \circ f_1$ such that $P\mathbf{u} = \mathbf{u}$ for $\mathbf{u} \in \operatorname{Im} K_B \circ f_1$ and $P\mathbf{u}' = 0$ for $\mathbf{u}' \in \operatorname{Im} K_B \circ f_2 + \operatorname{Im} H_B$. By applying the map P, Bob recovers the message $\mathbf{M}$. □

Assume that Bob knows K_B but does not know the form of H_B; i.e., there are several possible forms $H_{B,1}, \ldots, H_{B,d}$ as the candidate of H_B. Additionally, we assume that all possible forms $H_{B,1}, \ldots, H_{B,d}$ satisfy the condition of Proposition 1. In general, the map P used in the proof depends on the form of H_B. When the map P can be chosen commonly with $H_{B,1}, \ldots, H_{B,d}$, Bob can recover the message $\mathbf{M}$. Otherwise, Bob cannot recover it.

However, when the condition $\dim(\operatorname{Im} K_B \circ f_2 \cap \operatorname{Im} H_{B,i}) = 0$ holds in addition to the condition of Proposition 1 for $i = 1, \ldots, d$, Bob can detect the existence of contamination as follows. In this case, when $\mathbf{Y}_B$ does not belong to $\operatorname{Im} K_B \circ f_1 + \operatorname{Im} K_B \circ f_2$, Bob considers that a contamination exists. In other words, when we choose a linear function f_3 such that $\{\mathbf{y}_B \in \mathbb{F}_q^{m_3} | f_3(\mathbf{y}_B) = 0\} = \operatorname{Im} K_B \circ f_1 + \operatorname{Im} K_B \circ f_2$, the existence of a contamination can be detected by checking the condition $f_3(\mathbf{Y}_B) = 0$.

When the strategy α satisfies the uniqueness condition, Eve's recovery can be reduced to the case with $\mathbf{Z} = 0$ due to Theorem 1. Therefore, Eve can correctly recover the message $\mathbf{M}$ if and only if $\dim \operatorname{Im} K_E \circ f_1 = \ell$ and $\dim(\operatorname{Im} K_E \circ f_1 \cap \operatorname{Im} K_E \circ f_2) = 0$.

For the amount of information leakage, the papers [28] (Theorem 2), and [29] (Corollary 3.3 and (25)) stated the following relation in a slightly different way.

Proposition 2. *Information leakage to Eve can be evaluated as* $I(\mathbf{M};\mathbf{Y}_E)[0] = (\log q)(\dim \operatorname{Im} K_E \circ f_1 - \dim(\operatorname{Im} K_E \circ f_1 \cap \operatorname{Im} K_E \circ f_2))$. *In particular,* $I(\mathbf{M};\mathbf{Y}_E)[0] = 0$ *if and only if* $\dim \operatorname{Im} K_E \circ f_1 = \dim(\operatorname{Im} K_E \circ f_1 \cap \operatorname{Im} K_E \circ f_2)$.

Proof. Consider the case with $\alpha = 0$. $H(\mathbf{Y}_E) = (\log q)\dim(\mathrm{Im}\, K_E \circ f_1 + \mathrm{Im}\, K_E \circ f_2)$ and $H(\mathbf{Y}_E|\mathbf{M}) = (\log q)\dim \mathrm{Im}\, K_E \circ f_2$. Hence, $I(\mathbf{M};\mathbf{Y}_E)[0] = (\log q)\dim(\mathrm{Im}\, K_E \circ f_1 + \mathrm{Im}\, K_E \circ f_2) - (\log q)\dim \mathrm{Im}\, K_E \circ f_2 = (\log q)(\dim \mathrm{Im}\, K_E \circ f_1 - \dim(\mathrm{Im}\, K_E \circ f_1 \cap \mathrm{Im}\, K_E \circ f_2))$. □

Therefore, using Proposition 2, we can evaluate the amount of leaked information even for general strategy α.

To check the condition $\dim \mathrm{Im}\, K_E \circ f_1 = \dim(\mathrm{Im}\, K_E \circ f_1 \cap \mathrm{Im}\, K_E \circ f_2)$, we introduce two matrices $A_1 \in \mathbb{F}_q^{m_6 \times \ell}$ and $A_2 \in \mathbb{F}_q^{m_6 \times k}$ by $K_E \circ f_1(\mathbf{m}) = A_1\mathbf{m}$ for $\mathbf{m} \in \mathbb{F}_q^\ell$ and $K_E \circ f_2(\mathbf{l}) = A_2\mathbf{l}$ for $\mathbf{l} \in \mathbb{F}_q^k$. Then, we define m_6 low vectors $\mathbf{v}_i$ for $i = 1, \ldots, m_6$ of the matrix $A := (A_1 A_2)$. Considering an equivalent condition to $\dim \mathrm{Im}\, K_E \circ f_1 = \dim(\mathrm{Im}\, K_E \circ f_1 \cap \mathrm{Im}\, K_E \circ f_2)$, we have the following corollary.

Corollary 1. *$I(\mathbf{M};\mathbf{Y}_E)[0] = 0$ if and only if there does not exist a vector $(b_1, \ldots, b_{m_6}) \in \mathbb{F}_q^{m_6}$ such that $\sum_{i=1}^{m_6} b_i \mathbf{v}_i$ has a form $(\mathbf{m}, \underbrace{0, \ldots, 0}_{k})$ with $\mathbf{m} \neq 0 \in \mathbb{F}_q^\ell$.*

2.3. Construction of K_B, K_E from Concrete Network Model

Next, we discuss how we can obtain the generic passive attack model (1) from a concretely structured network coding, i.e., communications identified by directed edges and linear operations by parties identified by nodes. We consider the unicast setting of network coding on a network, which is given as a directed graph (V, E), where the set $V := \{v(1), \ldots, v(m_2)\}$ of vertices expresses the set of nodes and the set $E := \{e(1), \ldots, e(m_1)\}$ of edges expresses the set of communication channels, where a communication channel means a packet in network engineering; i.e., a single communication channel can transmit single character in $\mathbb{F}_q$. In the following, we identify the set E with $\{1, \ldots, m_1\}$; i.e, we identify the index of an edge with the edge itself. Here, the directed graph (V, E) is not necessarily acyclic. When a channel transmits information from a node $v(i) \in V$ to another node $v(i') \in V$, it is written as $(v(i), v(i')) \in E$.

In the single transmission, the source node has several elements of $\mathbb{F}_q$ and sends each of them via its outgoing edges in the order of assigned number of edges. Each intermediate node keeps received information via incoming edges. Then, for each outgoing edge, the intermediate node calculates one element of $\mathbb{F}_q$ from previously received information, and sends it via the outgoing edge. That is, every outgoing piece of information from a node $v(i)$ via a channel $e(j)$ depends only on the information coming into the node $v(i)$ via channels $e(j')$ such that $j' < j$. The operations on all nodes are assumed to be linear on the finite field $\mathbb{F}_q$ with prime power q. Bob receives the information $\mathbf{Y}_B$ in $\mathbb{F}_q^{m_4}$ on the edges of a subset $E_B := \{e(\zeta_B(1)), \ldots, e(\zeta_B(m_4))\} \subset E$, where ζ_B is a strictly increasing function from $\{1, \ldots, m_4\}$ to $\{1, \ldots, m_1\}$. Let $\tilde{X}_j$ be the information on the edge $e(j)$. In the following, we describe the information on the $m_7 = m_1 - m_3$ edges that are not directly linked to the source node because m_3 expresses the number of Alice's input symbols. When the edge $e(j)$ is an outgoing edge of the node $v(i)$, the information $\tilde{X}_j$ is given as a linear combination of the information on the edges coming into the node $v(i)$. We chose an $m_1 \times m_1$ matrix $\theta = (\theta_{j,j'})$ such that $\tilde{X}_j = \sum_{j'} \theta_{j,j'} \tilde{X}_{j'}$, where $\theta_{j,j'}$ is zero unless $e(j')$ is an edge incoming to $v(i)$. The matrix θ is the coefficient matrix of this network.

Now, from causality, we can assume that each node makes the transmissions on the outgoing edges in the order of the numbers assigned to the edges. At the first stage, all m_3 information generated at the source node is directly transmitted via $e(1), \cdots e(m_3)$ respectively. Then, at time j, the information transmission on the edge $e(j + m_3)$ is done. Hence, naturally, we impose the condition

$$\theta_{j,j'} = 0 \text{ for } j' \geq j, \tag{5}$$

which is called the partial time-ordered condition for θ. Then, to describe the information on m_7 edges that is not directly linked to the source node, we define m_7 $m_1 \times m_1$ matrices $M_1, \ldots, M_{m_7}$. The j-th $m_1 \times m_1$ matrix M_j gives the information on the edge $e(j + m_3)$ as a function of the information on edges $\{e(j')\}_{1 \leq j' \leq m_1}$ at time j. The $j + m_3$-th row vector of the matrix M_j is defined by $[\theta_{j+m_3,j'}]_{1 \leq j' \leq m_1}$.

The remaining part of M_j, i.e., the i-th row vector for $i \neq j + m_3$, is defined by $[\delta_{i,j'}]_{1 \le j' \le m_1}$ and $\delta_{i,j'}$ is the Kronecker delta. Since $\sum_{i=1}^{m_3} (M_j \cdots M_1)_{j',i} X_i$ expresses the information on edge $e(j')$ at time j, we have

$$Y_{B,j} = \sum_{i=1}^{m_3} (M_{m_7} \cdots M_1)_{\zeta_B(j),i} X_i. \tag{6}$$

While the output of the matrix $M_{m_7} \cdots M_1$ takes values in $\mathbb{F}_q^{m_1}$, we focus the projection P_B to the subspace $\mathbb{F}_q^{m_4}$ that corresponds to the m_4 components observed by Bob. That is, P_B is a $m_4 \times m_1$ matrix to satisfy $P_{B;i,j} = \delta_{\zeta_B(i),j}$. Similarly, we use the projection P_A (an $m_1 \times m_3$ matrix) as $P_{A;i,j} = \delta_{i,j}$. Due to (6), the matrix $K_B := P_B M_{m_7} \cdots M_1 P_A$ satisfies the first equation in (1).

The malicious adversary, Eve, wiretaps the information $\mathbf{Y}_E$ in $\mathbb{F}_q^{m_6}$ on the edges of a subset $E_E := \{e(\zeta_E(1)), \ldots, e(\zeta_E(m_6))\} \subset E$, where ζ_E is a strictly increasing function from $\{1, \ldots, m_6\}$ to $\{1, \ldots, m_1\}$. Similar to (6), we have

$$Y_{E,j} = \sum_{i=1}^{m_3} (M_{m_7} \cdots M_1)_{\zeta_E(j),i} X_i. \tag{7}$$

We employ the projection P_E (an $m_6 \times m_1$ matrix) to the subspace $\mathbb{F}_q^{m_6}$ that corresponds to the m_6 components eavesdropped by Eve. That is, $P_{E;i,j} = \delta_{\zeta_E(i),j}$. Then, we obtain the matrix K_E as $P_E M_{m_7} \cdots M_1 P_A$. Due to (6), the matrix $K_E := P_E M_{m_7} \cdots M_1 P_A$ satisfies the second equation in (1).

In summary the topology and dynamics (operations on the intermediate nodes) of the network, including the places of attached edges decides the graph (V, E), the coefficients $\theta_{i,j}$, and functions ζ_B, ζ_E, uniquely give the two matrices K_B and K_E. Section 2.6 gives an example for this model. Here, we emphasize that we do not assume the acyclic condition for the graph (V, E). We can use this relaxed condition because we have only one transmission in the current discussion. That is, due to the partial time-ordered condition for θ, we can uniquely define our matrices K_B and K_E, in a similar way to [30] (Section V-B; Λ of Ahlswede–Cai–Li–Yeung corresponds to the number of edges that are not connected to the source node in our paper.) However, when the graph has a cycle and we have n transmissions, there is a possibility of a correlation with the delayed information that is dependent on the time ordering. As a result, it is difficult to analyze secrecy for the cyclic network coding.

2.4. Construction of H_B, H_E from a Concrete Network Model

We identify the wiretap and addition model from a concrete network structure. We assume that Eve injects the noise in a part of edges $E_A \subset E$ and eavesdrops the edges E_E.

The elements of the subset E_A are expressed as $E_A = \{e(\eta(1)), \ldots, e(\eta(m_5))\}$ by using a function η from $\{1, \ldots, m_5\}$ to $\{1, \ldots, m_1\}$, where the function η is not necessarily monotonically increasing function. To give the matrices H_B and H_E, while modifying the matrix M_j, we define the new matrix M'_j as follows The $j + m_3$-th row vector of the new matrix M'_j is defined by $[\theta_{j+m_3,j'} + \delta_{j+m_3,j'}]_{1 \le j' \le m_1}$. The remaining part of M'_j, i.e., the i-th row vector for $i \neq j + m_3$, is defined by $[\delta_{i,j'}]_{1 \le j' \le m_1}$. Since $\sum_{i=1}^{m_3} (M_j \cdots M_1)_{j',i} X_i + \sum_{i'=1}^{m_5} (M'_j \cdots M'_1)_{j',\eta(i')} Z_{i'}$ expresses the information on edge $e(j')$ at time j, we have

$$Y_{B,j} = \sum_{i=1}^{m_3} (M_{m_7} \cdots M_1)_{\zeta_B(j),i} X_i + \sum_{i'=1}^{m_5} (M'_{m_7} \cdots M'_1)_{\zeta_B(j),\eta(i')} Z_{i'} \tag{8}$$

$$Y_{E,j} = \sum_{i=1}^{m_3} (M_{m_7} \cdots M_1)_{\zeta_E(j),i} X_i + \sum_{i'=1}^{m_5} (M'_{m_7} \cdots M'_1 - I)_{\zeta_E(j),\eta(i')} Z_{i'}. \tag{9}$$

When Eve eavesdrops the edges $E_E \cap E_A$, she obtains the information on $E_E \cap E_A$ before her noise injection. Hence, to express her obtained information on $E_E \cap E_A$, we need to subtract her injected information on $E_E \cap E_A$. Hence, we need $-I$ in the second term of (9). We introduce the projection

$P_{E,A}$ (an $m_1 \times m_5$ matrix) as $P_{E,A;i,j} = \delta_{i,\eta(j)}$. Due to (8) and (9), the matrices $H_B := P_B M'_{m_7} \cdots M'_1 P_{E,A}$ and $H_E := P_E (M'_{m_7} \cdots M'_1 - I) P_{E,A}$ satisfy conditions (2) with the matrices K_B and K_E, respectively. This model (K_B, K_E, H_B, H_E) to give (2) is called the wiretap and addition model determined by (V, E) and (E_E, E_A, θ), which expresses the topology and dynamics.

2.5. Strategy and Order of Communication

To discuss the active attack, we see how the causal condition for the subsets $\{w_i\}_{1,\ldots,m_5}$ follows from the network topology in the wiretap and addition model. We choose the domain index subsets $\{w_i\}_{1 \le i \le m_5}$ for α; i.e., Eve chooses the added error Z_i on the edge $e(\eta(i)) \in E_A$ as a function α_i of the vector $[Y_{E,j}]_{j \in w_i}$. Since the order of Eve's attack is characterized by the function η from $\{1, \ldots, m_5\}$ to $E_A \subset \{1, \ldots, m_1\}$, we discuss what condition for the pair $(\eta, \{w_i\}_i)$ guarantees the causal condition for the subsets $\{w_i\}_i$.

First, one may assume that the tail node of the edge $e(j)$ sends the information to the edge $e(j)$ after the head node of the edge $e(j-1)$ receives the information to the edge $e(j-1)$. Since this condition determines the order of Eve's attack, the function η must be a strictly increasing function from $\{1, \ldots, m_5\}$ to $\{1, \ldots, m_1\}$. Additionally, due to this time ordering, the subset w_i needs to be $\{j | \eta(i) \ge \zeta_E(j)\}$ or its subset. We call these two conditions the full time-ordered condition for the function η and the subsets $\{w_i\}_i$. Since the function η is strictly increasing, condition (A2) for the causal condition holds. Since the relation (5) implies that $M'_{m_7} \cdots M'_1 - I$ is a lower triangular matrix with zero diagonal elements, the strictly increasing property of η yields that

$$H_{E;j,i} = 0 \text{ when } \eta(i) \ge \zeta_E(j), \tag{10}$$

which implies condition (A1) for the causal condition. In this way, the full time-ordered condition for the function η and the subsets $\{w_i\}_i$ satisfies the causal condition.

However, the full time ordered condition does not hold in general, even when we reorder the numbers assigned to the edges. That is, if the network is not well synchronized, Eve can make an attack across several channels; i.e., it is possible that Eve might intercept (i.e., wiretap and contaminate) the information of an edge before the head node of the previous edge receives the information on the edge. Hence, we consider the case when the partial time-ordered condition holds, but the full time-ordered condition does not necessarily hold. (For an example, we consider the following case. Eve gets the information on the first edge. Then, she gets the information on the second edge before she hands over the information on the first edge to the tail node of the first edge. In this case, she can change the information on the first edge based on the information on the first and second edges. Then, the time-ordered condition (10) does not hold.) That is, the function η from $\{1, \ldots, m_5\}$ to E is injective but is not necessarily monotonically increasing. Given the matrix θ, we define the function $\gamma_\theta(j) := \min_{j'} \{j' | \theta_{j',j} \ne 0\}$. Here, when no index j' satisfies the condition $\theta_{j',j} \ne 0$, $\gamma_\theta(j)$ is defined to be $m_1 + 1$. Then, we say that the function η and the subsets $\{w_i\}_i$ are admissible under θ when $\{e(k) | k \in \mathrm{Im}\, \eta\} = E_A$, the subsets $\{w_i\}_i$ satisfy condition (A2) for the causal condition, and any element $j \in w_i$ satisfies

$$\zeta_E(j) < \gamma_\theta(\eta(i)). \tag{11}$$

Here, $\mathrm{Im}\, \eta$ expresses the image of the function η. The condition (11) and the condition (5) imply the following condition; for $j \in w_i$, there is no sequence $\zeta_E(j) = j_1 > j_2, \ldots > j_l = \eta(i)$ such that

$$\theta_{j_i, j_{i+1}} \ne 0. \tag{12}$$

This condition implies condition (A1) for the causal condition. Since the admissibility under θ is natural, even when the full time-ordered condition does not hold, the causal condition can be naturally derived.

Given two admissible pairs $(\eta, \{w_i\}_i)$ and $(\eta', \{w'_i\}_i)$, we say that the pair $(\eta, \{w_i\}_i)$ is superior to $(\eta', \{w'_i\}_i)$ for Eve when $w'_{\eta'^{-1}(j)} \subset w_{\eta^{-1}(j)}$ for any $j \in E_A$. Now, we discuss the optimal choice of $(\eta, \{w_i\}_i)$ in this sense when E_A is given. That is, we choose the subset w_i as large as possible under the admissibility under θ. Then, we choose the bijective function η_o from $\{1, \ldots, m_5\}$ to E_A such that $\gamma_\theta \circ \eta_o$ is monotonically increasing. Then, we define $w_{o,i} := \{j | \zeta_E(j) < \gamma_\theta(\eta_o(i))\}$, which satisfies the admissibility under θ. conditions (A1) and (A2) for the causal condition. Further, when the pair $(\eta, \{w_i\}_i)$ is admissible under θ, the condition (11) implies $w_{\eta^{-1}(j)} \subset w_{o,\eta_o^{-1}(j)}$ for $j \in E_A$; i.e., $w_{o,i}$ is the largest subset under the admissibility under θ. Hence, we obtain the optimality of $(\eta_o, \{w_{o,i}\}_i)$. Although the choice of η_o is not unique, the choice of $w_{o,\eta_o^{-1}(j)}$ for $j \in E_A$ is unique.

2.6. Secrecy in Concrete Network Model

In this subsection, as an example, we consider the network given in Figures 1 and 2, which shows that our framework can be applied to the network without synchronization. Alice sends the variables $X_1, \ldots, X_4 \in \mathbb{F}_q$ to nodes $v(1), v(2), v(3)$, and $v(4)$ via the edges $e(1), e(2), e(3)$, and $e(4)$, respectively. The edges $e(5), e(6), e(8), e(10)$ send the elements received from the edges $e(1), e(5), e(5), e(8)$, respectively. The edges $e(7)$, $e(9)$, and $e(11)$ send the sum of two elements received from the edge pairs $(e(2), e(5))$, $(e(3), e(6))$, and $(e(4), e(8))$, respectively.

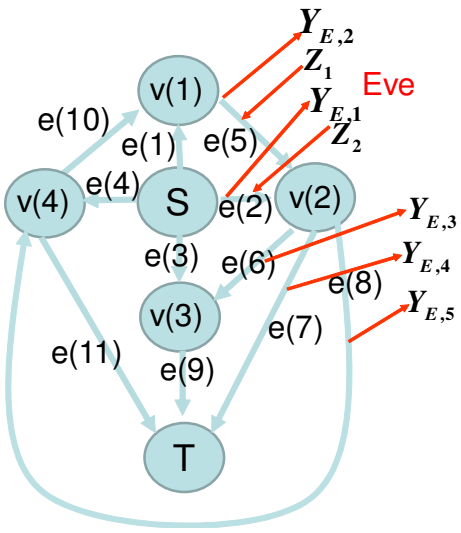

Figure 1. Network of Section 2.6 with name of edges.

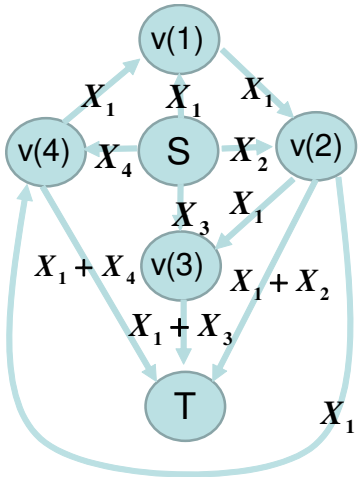

Figure 2. Network of Section 2.6 with network flow.

Bob receives elements via the edges $e(7), e(9)$, and $e(11)$, which are written as $Y_{B,1}, Y_{B,2}$, and $Y_{B,3}$, respectively. Then, the matrix K_B is given as

$$K_B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}. \tag{13}$$

Then, $m_3 = 4$ and $m_4 = 3$.

Now, we assume that Eve eavesdrops the edges $e(2), e(5), e(6), e(7)$, and $e(8)$, i.e., all edges connected to $v(2)$, and contaminates the edge $e(2), e(5)$. Then, we set $\zeta_B(1) = 7, \zeta_B(2) = 9, \zeta_B(3) = 11$ and $\zeta_E(1) = 2, \zeta_E(2) = 5, \zeta_E(3) = 6, \zeta_E(4) = 7, \zeta_E(5) = 8$. Eve can choose the function η as

$$\eta(1) = 5, \quad \eta(2) = 2 \tag{14}$$

while $\eta(1) = 2, \eta(2) = 5$ is possible. In the following, we choose (14). Since $\gamma_\theta(2) = 7$ and $\gamma_\theta(5) = 6$, the subsets w_i are given as

$$w_1 := w_{o,1} = \{1, 2\}, \quad w_2 := w_{o,2} = \{1, 2, 3\} \tag{15}$$

This case satisfies conditions (A1) and (A2). Hence, this model satisfies the causal condition. Lemma 1 guarantees that any strategy also satisfies the uniqueness condition.

We denote the observed information on the edges $e(2), e(5), e(6), e(7)$, and $e(8)$ by $Y_{E,1}, Y_{E,2}, Y_{E,3}, Y_{E,4}$, and $Y_{E,5}$. As in Figure 1, Eve adds Z_1 and Z_2 in edges $e(2)$ and $e(5)$. Then, the matrices H_B, K_E, and H_E are given as

$$H_B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad K_E = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad H_E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{16}$$

In this case, to keep the secrecy of the message to be transmitted, Alice and Bob can use coding as follows. When Alice's message is $M \in \mathbb{F}_q$, Alice prepares scramble random number $L_1, L_2, L_3 \in \mathbb{F}_q$. These variables are assumed to be subject to the uniform distribution independently. She encodes them as $X_i = L_i$ for $i = 1, \ldots, 3$ and $X_4 = -M + L_1 + L_2 + L_3$. As shown in the following, under this code, Eve cannot obtain any information for M, even though she makes active attack. Due to Theorem 1, it is sufficient to show the secrecy when $Z_i = 0$. Since Eve's information is $Y_{E,1} = X_2, Y_{E,2} = X_1, Y_{E,3} = X_1, Y_{E,4} = X_1 + X_2$, and $Y_{E,5} = X_1$, the matrix A given in Section 2.2 is

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{17}$$

Thus, Proposition 2 guarantees that Eve cannot obtain any information for the message M.

Indeed, the above attack can be considered as the following. Eve can eavesdrop all edges connected to the intermediate node $v(2)$ and contaminate all edges incoming to the intermediate node $v(2)$. Hence, it is natural to assume that Eve similarly eavesdrops and contaminates at another intermediate node $v(i)$. That is, Eve can eavesdrop all edges connected to the intermediate node $v(i)$ and contaminate all edges incoming to the intermediate node $v(i)$. For all nodes $v(i)$, this code has the same secrecy against the above Eve's attack for node $v(i)$.

Furthermore, the above code has the secrecy even when the following attack.

(B1) Eve eavesdrops one of three edges $e(7), e(9)$, and $e(11)$ connected to the sink node, and eavesdrops and contaminates one of the remaining eight edges $e(1), e(2), e(3), e(4), e(5), e(6), e(8)$, and $e(10)$ that are not connected to the sink node.

To apply Corollary 1 for analysis of the secrecy, we denote the low vector in Corollary 1 corresponding to the edge $e(i)$ by $\mathbf{v}_i$. Then, the vectors $\mathbf{v}_7$, $\mathbf{v}_9$, and $\mathbf{v}_{11}$ are $(0,1,1,0)$, $(0,1,0,1)$, and $(-1,2,1,1)$. The remaining vectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$, $\mathbf{v}_4$, $\mathbf{v}_5$, $\mathbf{v}_6$, $\mathbf{v}_8$, and $\mathbf{v}_{10}$ are $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$, $(-1,1,1,1)$, $(0,1,0,0)$, $(0,1,0,0)$, $(0,1,0,0)$, and $(0,1,0,0)$. Since any combination of the vector of the first group and the second group cannot be $(1,0,0,0)$ the combination of Corollary 1 and Theorem 2 guarantees that the secrecy holds under the above attack (B1).

2.7. A Problem in Error Detection in a Concrete Network Model

However, the network given in Figures 1 and 2 has the problem for the detection of the error in the following meaning. When Eve makes an active attack, Bob's recovering message is different from the original message due to the contamination. Further, Bob cannot detect the existence of the error in this case. It is natural to require the detection of the existence of the error when the original message cannot be recovered and the secrecy. As a special attack model, we consider the following scenario with the attack (B1).

(B2) Our node operations are fixed to the way as Figure 2.
(B3) The message set $\mathcal{M}$ and all information on all edges are $\mathbb{F}_2$.
(B4) The variables X_1, X_2, X_3, and X_4 are given as the output of the encoder. The encoder on the source node can be chosen, but is restricted to linear. It is allowed to use a scramble random number, which is an element of $\mathcal{L} := \mathbb{F}_2^k$ with a certain integer k. Formally, the encoder is given as a linear function from $\mathcal{M} \times \mathcal{L}$ to $\mathbb{F}_2^4$.
(B5) The decoder on the sink node can be chosen dependently of the encoder and independently of Eve's attack.

Then, it is impossible to make a pair of an encoder and a decoder such that the secrecy holds and Bob can detect the existence of error.

This fact can be shown as follows. In order to detect it, as discussed in Section 2.2, Alice needs to make an encoder such that the vector $(Y_{B,1}, Y_{B,2}, Y_{B,3})$ belongs to a linear subspace because the detection can be done only by observing that the vector does not belong to a certain linear subspace, which can be written as $\{(Y_{B,1}, Y_{B,2}, Y_{B,3}) | c_1 Y_{B,1} + c_2 Y_{B,2} + c_3 Y_{B,3} = 0\}$ with a non-zero vector $(c_1, c_2, c_3) \in \mathbb{F}_2^3$. That is, the encoder needs to be constructed so that the relation $c_1 Y_{B,1} + c_2 Y_{B,2} + c_3 Y_{B,3} = (c_1 + c_2 + c_3)X_1 + c_1 X_2 + c_2 X_3 + c_3 X_4 = 0$ holds unless Eve's injection is made. Since our field is $\mathbb{F}_2^3$, we have three cases. (C1) (c_1, c_2, c_3) is $(1,0,0)$, $(0,1,0)$, or $(0,0,1)$. (C2) (c_1, c_2, c_3) is $(1,1,0)$, $(0,1,1)$, or $(0,1,1)$. (C3) (c_1, c_2, c_3) is $(1,1,1)$. If we impose another linear condition, the transmitted information is restricted into a one-dimensional subspace, which means that the message M uniquely decides the vector $(Y_{B,1}, Y_{B,2}, Y_{B,3})$. Hence, if Eve eavesdrops one suitable variable among three variables $Y_{B,1}, Y_{B,2}$, and $Y_{B,3}$, Eve can infer the original message.

In the first case (C1), one of three variables $Y_{B,1}, Y_{B,2}$, and $Y_{B,3}$ is zero unless Eve's injection is made. When $Y_{B,1} = 0$, i.e., $(c_1, c_2, c_3) = (1,0,0)$, Bob can detect an error on the edge $e(5)$ or $e(2)$ because the error on $e(5)$ or $e(2)$ affects $Y_{B,1}$ so that $Y_{B,1}$ is not zero. However, Bob cannot detect any error on the edge $e(4)$ because the error does not affect $Y_{B,1}$. The same fact can be applied to the case when $Y_{B,2} = 0$. When $Y_{B,3} = 0$, Bob cannot detect any error on the edge $e(3)$ because the error does not affect $Y_{B,3}$.

In the second case (C2), two of three variables $Y_{B,1}, Y_{B,2}$, and $Y_{B,3}$ have the same value unless Eve's injection is made. When $Y_{B,1} = Y_{B,2}$, i.e., $(c_1, c_2, c_3) = (1,1,0)$, Bob can detect an error on the edge $e(2)$ or $e(3)$ because the error on $e(2)$ or $e(3)$ affects $Y_{B,1}$ or $Y_{B,2}$ so that $Y_{B,1} + Y_{B,2}$ is not zero. However, Bob cannot detect any error on the edge $e(4)$ because the error does not affect $Y_{B,1}$ or $Y_{B,2}$. Similarly, When $Y_{B,2} = Y_{B,3}$ ($Y_{B,1} = Y_{B,3}$), Bob cannot detect any error on the edge $e(2)$ ($e(3)$).

In the third case (C3), the relation $Y_{B,1} = Y_{B,2} + Y_{B,3}$ holds; i.e., $(c_1, c_2, c_3) = (1, 1, 1)$. Then, the linearity of the code implies that the message has the form $a_1 Y_{B,1} + a_2 Y_{B,2} + a_3 Y_{B,3}$. Due to the relation $Y_{B,1} = Y_{B,2} + Y_{B,3}$, the value $a_1 Y_{B,1} + a_2 Y_{B,2} + a_3 Y_{B,3} = (a_1 + a_2) Y_{B,2} + (a_1 + a_3) Y_{B,3}$ is limited to $Y_{B,1}$, $Y_{B,2}$, $Y_{B,3}$, or 0 because our field is $\mathbb{F}_2$. Since the message is not a constant, it is limited to one of $Y_{B,1}$, $Y_{B,2}$, or $Y_{B,3}$. Hence, when it is $Y_{B,1}$, Eve can obtain the message by eavesdropping the edge $e(7)$. In other cases, Eve can obtain the message in the same way.

To resolve this problem, we need to use this network multiple times. Hence, in the next section, we discuss the case with multiple transmission.

2.8. Wiretap and Replacement Model

In the above subsections, we have discussed the case when Eve injects the noise in the edges E_A and eavesdrops the edges E_E. In this subsection, we assume that $E_A \subset E_E$ and Eve eavesdrops the edges E_E and replaces the information on the edges E_A by other information. While this assumption implies $m_5 \le m_6$ and the image of η is included in the image of ζ_E, the function η does not necessarily equal the function ζ_E because the order that Eve sends her replaced information to the heads of edges does not necessarily equal the order that Eve intercepts the information on the edges. Additionally, this case belongs to general wiretap and addition model (2) as follows. Modifying the matrix M_j, we define the new matrix M''_j as follows. When there is an index i such that $\zeta_E(i) = j$, the $j + m_3$-th row vector of the new matrix M''_j is defined by $[\delta_{j+m_3,j'}]_{1 \le j' \le m_1}$ and the remaining part of M''_j is defined as the identity matrix. Otherwise, M''_j is defined to be M_j. Additionally, we define another matrix F as follows. The $\zeta_E(i)$-th row vector of the new matrix F is defined by $[\theta_{\zeta_E(i),j'}]_{1 \le j' \le m_1}$ and the remaining part of F is defined as the identity matrix. Hence, we have

$$Y_{B,j} = \sum_{i=1}^{m_3} (M''_{m_7} \cdots M''_1)_{\zeta_B(j),i} X_i + \sum_{i'=1}^{m_5} (M''_{m_7} \cdots M''_1)_{\zeta_B(j),\eta(i')} Z_{i'} \tag{18}$$

$$Y_{E,j} = \sum_{i=1}^{m_3} (F M''_{m_7} \cdots M''_1)_{\zeta_E(j),i} X_i + \sum_{i'=1}^{m_5} (F M''_{m_7} \cdots M''_1)_{\zeta_E(j),\eta(i')} Z_{i'}. \tag{19}$$

Then, we choose matrices K'_B, K'_E, H'_B, and H'_E as $K'_B := P_B M''_{m_7} \cdots M''_1 P_A$, $K'_E := P_E F M''_{m_7} \cdots M''_1 P_A$, $H'_B := P_B M''_{m_7} \cdots M''_1 P_E^T$, and $H'_E := P_E F M''_{m_7} \cdots M''_1 P_E^T$, which satisfy conditions (2) due to (18) and (19). This model (K'_B, K'_E, H'_B, H'_E) is called the wiretap and replacement model determined by (V, E) and (E_E, E_A, θ, η). Notice that the projections P_A, P_B, and P_E are defined in Section 2.3.

Next, we discuss the strategy α' under the matrices K'_B, K'_E, H'_B, and H'_E such that the added error Z_i is given as a function α'_i of the vector $[Y_{E,j}]_{j \in w_i}$. Since the decision of the injected noise does not depend on the results of the decision, we impose the causal condition defined in Definition 4 for the subsets w_i.

When the relation $j \in w_i$ holds with $\zeta_E(j) = \eta(i)$, a strategy α' on the wiretap and replacement model (K'_B, K'_E, H'_B, H'_E) determined by (V, E) and (E_E, θ) is written by another strategy α on the wiretap and addition model K_B, K_E, H_B, and H_E determined by (V, E) and (E_E, θ), which is defined as $\alpha_j([Y_{E,j'}]_{j' \in w_i}) := \alpha'_j([\hat{Y}_{E,j'}]_{j' \in w_i}) - Y_{E,j}$. In particular, due to the condition (5), the optimal choice $\eta_o, \{w_{o,i}\}$ under the partial time-ordered condition satisfies that the relation $j \in w_{o,i}$ holds with $\zeta_E(j) = \eta_o(i)$. That is, under the partial time-ordered condition, the strategy on the wiretap and replacement model can be written by another strategy on the wiretap and addition model.

However, if there is no synchronization among vertexes, Eve can inject the replaced information to the head of an edge before the tail of the edge sends the information to the edge. Then, the partial time-ordered condition does not hold. In this case, the relation $j \in w_i$ does not necessarily hold with $\zeta_E(j) = \eta(i)$. Hence, a strategy α' on the wiretap and replacement model (K'_B, K'_E, H'_B, H'_E) cannot be necessarily written as another strategy on the wiretap and addition model (K_B, K_E, H_B, H_E).

To see this fact, we discuss an example given in Section 2.6. In this example, the network structure of the wiretap and replacement model is given by Figure 3.

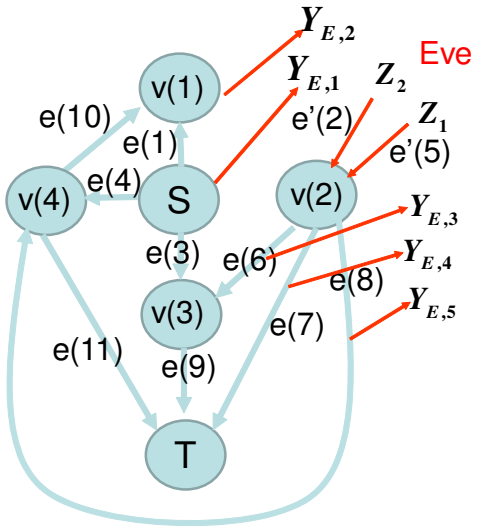

Figure 3. Network of Section 2.6 with the wiretap and replacement model. Eve injects the replaced information on the edges $e'(2)$ and $e'(5)$.

3. Multiple Transmission Setting

3.1. General Model

Now, we consider the n-transmission setting, where Alice uses the same network n times to send a message to Bob. Alice's input variable (Eve's added variable) is given as a matrix $X^n = (\mathbf{X}_1, \ldots, \mathbf{X}_n) \in \mathbb{F}_q^{m_3 \times n}$ (a matrix $Z^n = (\mathbf{Z}_1, \ldots, \mathbf{Z}_n) \in \mathbb{F}_q^{m_5 \times n}$), and Bob's (Eve's) received variable is given as a matrix $Y_B^n = (\mathbf{Y}_{B,1}, \ldots, \mathbf{Y}_{B,n}) \in \mathbb{F}_q^{m_4 \times n}$ (a matrix $Y_E^n = (\mathbf{Y}_{E,1}, \ldots, \mathbf{Y}_{E,n}) \in \mathbb{F}_q^{m_6 \times n}$). Then, we consider the model

$$Y_B^n = K_B X^n + H_B Z^n, \tag{20}$$
$$Y_E^n = K_E X^n + H_E Z^n, \tag{21}$$

whose realization in a concrete network will be discussed in Sections 3.2 and 3.3. Notice that the relations (20) and (21) with $H_E = 0$ (only the relation (20)) were treated as the starting point of the paper [20] (the papers [22–24]).

In this case, regarding n transmissions of one channel as n different edges, we consider the directed graph composed of nm_5 edges. Then, Eve's strategy α^n is given as nm_5 functions $\{\alpha_{i,l}\}_{1 \le i \le m_5, 1 \le l \le n}$ from Y_E^n to the respective components of Z^n. In this case, we extend the uniqueness condition to the n-transmission version.

Definition 3. *For any value of $K_E x^n$, there uniquely exists $y^n \in \mathbb{F}_q^{m_6 \times n}$ such that*

$$y^n = K_E x^n + H_E \alpha^n(y^n). \tag{22}$$

This condition is called the n-uniqueness condition.

Since we have n transmissions on each channel, the matrix θ is given as an $(nm_1) \times (nm_1)$ matrix. In the following, we see how the matrix θ is given and how the n-uniqueness condition is satisfied in a more concrete setting.

3.2. The Multiple Transmission Setting with Sequential Transmission

This section discusses how the model given in Section 3.1 can be realized in the case with sequential transmission as follows. Alice sends the first information $\mathbf{X}_1$. Then, Alice sends the second

information $\mathbf{X}_2$. Alice sequentially sends the information $\mathbf{X}_3, \ldots, \mathbf{X}_n$. Hence, when an injective function τ_E from $\{1, \ldots, m_1\} \times \{1, \ldots, n\}$ to $\{1, \ldots, nm_1\}$ gives the time ordering of nm_1 edges, it satisfies the condition

$$\tau_E(i, l) \le \tau_E(i', l') \text{ when } i \le i' \wedge l \le l'. \tag{23}$$

Here, we assume that the topology and dynamics of the network and the edge attacked by Eve do not change during n transmissions, which is called the stationary condition. All operations in intermediate nodes are linear. Additionally, we assume that the time ordering on the network flow does not cause any correlation with the delayed information like Figure 1 unless Eve's injection is made; i.e., the l-th information $\mathbf{Y}_{B,l}$ received by Bob is independent of $\mathbf{X}_1, \ldots, \mathbf{X}_{l-1}, \mathbf{X}_{l+1}, \ldots, \mathbf{X}_n$, which is called the independence condition. The independence condition means that there is no correlation with the delayed information. Due to the stationary and independence conditions, the $(nm_1) \times (nm_1)$ matrix θ satisfies that

$$\theta_{(i,l),(j,k)} = \bar{\theta}_{i,j} \delta_{k,l}, \tag{24}$$

where $\bar{\theta}_{i,j} := \theta_{(i,1),(j,1)}$. When the $m_1 \times m_1$ matrix $\bar{\theta}$ satisfies the partial time-ordered condition (5), due to (23) and (24), the $(nm_1) \times (nm_1)$ matrix θ satisfies the partial time-ordered condition (5) with respect to the time ordering τ_E. Since the stationary condition guarantees that the edges attacked by Eve do not change during n transmissions, the above condition for θ implies the model (20) and (21). This scenario is called the n-sequential transmission.

Since the independence condition is not so trivial, it is needed to discuss when it is satisfied. If the l-th transmission has no correlation with the delayed information of the previous transmissions for $l = 2, \ldots, n$, the independence condition holds. In order to satisfy the above independence condition, the acyclic condition for the network graph is often imposed. This is because any causal time ordering on the network flow does not cause any correlation with the delayed information and achieves the max-flow if the network graph has no cycle [31]. In other words, if the network graph has a cycle, there is a possibility that a good time ordering on the network flow that causes correlation with the delayed information. However, there is no relation between the relations (20) and (21) and the acyclic condition for the network graph, and the relations (20) and (21) directly depend on the time ordering on the network flow. That is, the acyclic condition for the network graph is not equivalent to the existence of the effect of delayed information. Indeed, if we employ breaking cycles on intermediate nodes ([31] Example 3.1), even when the network graph has cycles, we can avoid any correlation with the delayed information. (To handle a time ordering with delayed information, one often employs a convolution code [32]. It is used in sequential transmission, and requires synchronization among all nodes. Additionally, all the intermediate nodes are required to make a cooperative coding operation under the control of the sender and the receiver. If we employ breaking cycles, we do not need such synchronization and avoid any correlation with the delayed information.) Additionally, see the example given in Section 3.5.

To extend the causality condition, we focus on the domain index subsets $\{w_{i,l}\}_{1 \le i \le m_5, 1 \le l \le n}$ of $\{1, \ldots, m_6\} \times \{1, \ldots, n\}$ for Eve's strategy $\alpha^n = \{\alpha_{i,l}\}_{1 \le i \le m_5, 1 \le l \le n}$. Then, we define the causality condition under the order function τ_E.

Definition 4. *We say that the domain index subsets $\{w_{i,l}\}_{i,l}$ satisfy the n-causal condition under the order function τ_E and the function η from $\{1, \ldots, m_5\}$ to $\{1, \ldots, m_1\}$ when the following two conditions hold:*

(A1') *The relation $H_{E;j,i} = 0$ holds for $(j, l) \notin w_{i,l}$.*
(A2') *The relation $w_{i,l} \subseteq w_{i',l'}$ holds when $\tau_E(\eta(i), l) \le \tau_E(\eta(i'), l')$.*

Next, we focus on the domain index subsets $\{w_{i,l}\}_{i,l}$ and the function η from $\{1, \ldots, m_5\}$ to $\{1, \ldots, m_1\}$. We say that the pair $(\eta, \{w_{i,l}\}_{i,l})$ are n-admissible under $\bar{\theta}$ under the order function τ_E

when $\{e(k)|k \in \mathrm{Im}\,\eta\} = E_A$, the subsets $\{w_{i,l}\}_{i,l}$ satisfy condition (A2′) for the n causal condition, and any element $(j,l') \in w_{i,l}$ satisfies

$$\tau_E(\zeta_E(j),l') < \gamma_{\bar{\theta}}(\eta(i),l). \tag{25}$$

where the function $\gamma_{\bar{\theta}}$ is defined as

$$\gamma_{\bar{\theta}}(j,l) := \min_{j'}\{\tau_E(j',l)|\bar{\theta}_{j',j} \neq 0\}. \tag{26}$$

Here, when no index j' satisfies the condition $\bar{\theta}_{j',j} \neq 0$, $\gamma_{\bar{\theta}}(j,l)$ is defined to be nm_1+1. In the same way as Section 2.5, we find that the n-admissibility of the pair $(\eta,\{w_{i,l}\}_{i,l})$ implies the n-causal condition under τ_E and η for the domain index subsets $\{w_{i,l}\}_{i,l}$.

Given two n-admissible pairs $(\eta,\{w_{i,l}\}_{i,l})$ and $(\eta',\{w'_{i,l}\}_{i,l})$, we say that the pair $(\eta,\{w_{i,l}\}_{i,l})$ is superior to $(\eta',\{w'_{i,l}\}_{i,l})$ for Eve when $w'_{\eta'^{-1}(j),l} \subset w_{\eta^{-1}(j),l}$ for $j \in E_A$ and $l = 1,\ldots,n$. Then, we choose the bijective function $\tau_{E,\eta}$ from $\{1,\ldots,m_5\}\times\{1,\ldots,n\}$ to $\{1,\ldots,nm_5\}$ such that $\gamma_{\bar{\theta}}\circ\eta\circ\tau_{E,\eta}^{-1}$ is monotonically increasing, where $\gamma_{\bar{\theta}}\circ\eta$ is defined as $\gamma_{\bar{\theta}}\circ\eta(i,l) = \gamma_{\bar{\theta}}(\eta(i),l)$. The function $\tau_{E,\eta}$ expresses the order of Eve's contamination. Then, we define $w_{\eta,i,l} := \{(j,l')|\tau_E(\zeta_E(j),l') < \gamma_{\bar{\theta}}(\eta(i),l)\}$, which satisfies the n-admissibility under $\bar{\theta}$ and the order function τ_E.

Further, when the pair $(\eta',\{w_{i,l}\}_{i,l})$ is n-admissible under $\bar{\theta}$ and τ_E, the condition (25) implies $w_{\eta'^{-1}(j),l} \subset w_{\eta,\eta^{-1}(j),l}$ for $j \in E_A$ and $l = 1,\ldots,n$; i.e., $w_{\eta,i,l}$ is the largest subset under the n admissibility under $\bar{\theta}$ and τ_E. Hence, we obtain the optimality of $(\eta,\{w_{\eta,i,l}\}_{i,l})$ when $\bar{\theta}$, τ_E, and E_A are given. Although the choice of η is not unique, the choice of $w_{\eta,\eta^{-1}(j),l}$ for $j \in E_A$ and $l = 1,\ldots,n$ is unique when $\bar{\theta}$, τ_E, and E_A are given.

In the same way as Lemma 1, we find that the n-causal condition with sequential transmission guarantees the n-uniqueness condition as follows.

Lemma 2. *When a strategy α for the n-sequential transmission has domain index subsets to satisfy the n-causal condition, the strategy α satisfies the n-uniqueness condition.*

Proof. Consider a big graph composed of nm_1 edges $\{e(i,l)\}_{1\le i\le m_1,1\le l\le n}$ and nm_2 vertecies $\{v(j,l)\}_{1\le j\le m_2,1\le l\le n}$. In this big graph, the coefficient matrix is given in (24). We assign the nm_1 edges the number $\tau_E(i,l)$. The n-causal and n-uniqueness conditions correspond to the causal and uniqueness conditions of this big network, respectively. Hence, Lemma 1 implies Lemma 2. □

3.3. Multiple Transmission Setting with Simultaneous Transmission

We consider anther scenario to realize the model given in Section 3.1. Usually, we employ an error correcting code for the information transmission on the edges in our graph. For example, when the information transmission is done by wireless communication, an error correcting code is always applied. Now, we assume that the same error correcting code is used on all the edges. Then, we set the length n to be the same value as the transmitted information length of the error correcting code. In this case, n transmissions are done simultaneously in each edge. Each node makes the same node operation for n transmissions, which implies the condition (24) for the $(nm_1)\times(nm_1)$ matrix θ. Then, the relations (20) and (21) hold because the delayed information does not appear. This scenario is called the n-simultaneous transmission.

In fact, when we focus on the mathematical aspect, the n-simultaneous transmission can be regarded as a special case of the n-sequential transmission. In this case, the independence condition always holds even when the network has a cycle. Further, the n-uniqueness condition can be derived in a simpler way without discussing the n-causal condition as follows.

In this scenario, given a function η from $\{1,\ldots,m_5\}$ to $E_A \subset \{1,\ldots,m_1\}$, Eve chooses the added errors $(Z_{i,1},\ldots,Z_{i,n}) \in \mathbb{F}_q^n$ on the edge $e(\eta(i)) \in E_A$ as a function α_i of the vector $[Y_{E,j}]_{j\in w_i}$ with subsets

$\{w_i\}_{1\le i\le m_5}$ of $\{1,\dots,m_6\}$. Hence, in the same way as the single transmission, domain index subsets for α are given as subsets $w_i \subset \{1,\dots,m_6\}$ for $i \in \{1,\dots,m_5\}$. In the same way as Lemma 1, we have the following lemma.

Lemma 3. *When a strategy α for the n-simultaneous transmission has domain index subsets to satisfy the causal condition, the strategy α satisfies the n-uniqueness condition.*

In addition, the wiretap and replacement model in this setting can be introduced for the n-sequential transmission and the n-simultaneous transmission in the same way as Section 2.8.

3.4. Non-Local Code and Reduction Theorem

Now, we assume only the model (20) and (21) and the n-uniqueness condition. Since the model (20) and (21) is given, we manage only the encoder in the sender and the decoder in the receiver. Although the operations in the intermediate nodes are linear and operate only on a single transmission, the encoder and the decoder operate across several transmissions. Such a code is called a non-local code to distinguish operations over a single transmission. Here, we formulate a non-local code to discuss the secrecy. Let $\mathcal{M}$ and $\mathcal{L}$ be the message set and the set of values of the scramble random number, which is often called the private randomness. Then, an encoder is given as a function ϕ_n from $\mathcal{M}\times\mathcal{L}$ to $\mathbb{F}_q^{m_3\times n}$, and the decoder is given as ψ_n from $\mathbb{F}_q^{m_4\times n}$ to $\mathcal{M}$. Here, the linearity for ϕ_n and ψ_n is not assumed. That is, the decoder does not use the scramble random number L because it is not shared with the decoder. Our non-local code is the pair (ϕ_n,ψ_n), and is denoted by Φ_n. Then, we denote the message and the scramble random number as M and L. The cardinality of $\mathcal{M}$ is called the size of the code and is denoted by $|\Phi_n|$. More generally, when we focus on a sequence $\{l_n\}$ instead of $\{n\}$, an encoder ϕ_n is a function from $\mathcal{M}\times\mathcal{L}$ to $\mathbb{F}_q^{m_3\times l_n}$, and the decoder ψ_n is a function from $\mathbb{F}_q^{m_4\times l_n}$ to $\mathcal{M}$.

Here, we treat K_B, K_E, H_B, and H_E as deterministic values, and denote the pairs (K_B,K_E) and (H_B,H_E) by $\boldsymbol{K}$ and $\boldsymbol{H}$, respectively, while Alice and Bob might not have the full information for K_E, H_B, and H_E. Additionally, we assume that the matrices $\boldsymbol{K}$ and $\boldsymbol{H}$ are not changed during transmission. In the following, we fix $\Phi_n,\boldsymbol{K},\boldsymbol{H},\alpha^n$. As a measure of the leaked information, we adopt the mutual information $I(M;Y_E^n,Z^n)$ between M and Eve's information Y_E^n and Z^n. Since the variable Z^n is given as a function of Y_E^n, we have $I(M;Y_E^n,Z^n) = I(M;Y_E^n)$. Since the leaked information is given as a function of $\Phi_n,\boldsymbol{K},\boldsymbol{H},\alpha^n$ in this situation, we denote it by $I(M;\mathbf{Y}_E^n)[\Phi_n,\boldsymbol{K},\boldsymbol{H},\alpha^n]$.

Definition 5. *When we always choose $Z^n = 0$, the attack is the same as the passive attack. This strategy is denoted by $\alpha^n = 0$.*

When $\boldsymbol{K},\boldsymbol{H}$ are treated as random variables independent of M, L, the leaked information is given as the expectation of $I(M;Y_E^n)[\Phi_n,\boldsymbol{K},\boldsymbol{H},\alpha^n]$. This probabilistic setting expresses the following situation. Eve cannot necessarily choose edges to be attacked by herself. However, she knows the positions of the attacked edges, and chooses her strategy depending on the attacked edges.

Remark 1. *It is better to remark that there are two kinds of formulations in network coding, even when the network has only one sender and one receiver. Many papers [1,8,9,28,29] adopt the formulation, where the users can control the coding operation in intermediate nodes. However, this paper adopts another formulation, in which the non-local coding operations are done only for the input variable $\mathbf{X}$ and the output variable $\mathbf{Y}_B$ like the papers [7,14,20,22–24]. In contrast, all intermediate nodes make only linear operations over a single transmission, which is often called local encoding in [22–24]. Since the linear operations in intermediate nodes cannot be controlled by the sender and the receiver, this formulation contains the case when a part of intermediate nodes do not work and output 0 always.*

In the former setting, it is often allowed to employ the private randomness in intermediate nodes. However, we adopt the latter setting; i.e., no non-local coding operation is allowed in intermediate nodes, and each intermediate node is required to make the same linear operation on each alphabet. That is, the operations in

intermediate nodes are linear and are not changed during n transmissions. The private randomness is not employed in intermediate nodes.

Now, we have the following reduction theorem.

Theorem 2 (Reduction theorem)**.** *When the triplet* $(\boldsymbol{K}, \boldsymbol{H}, \alpha^n)$ *satisfies the uniqueness condition, Eve's information* $Y_E^n(\alpha^n)$ *with strategy* α^n *can be calculated from Eve's information* $Y_E^n(0)$ *with strategy* 0 *(the passive attack), and* $Y_E^n(0)$ *is also calculated from* $Y_E^n(\alpha^n)$*. Hence, we have the equation*

$$I(M; Y_E^n)[\Phi_n, \boldsymbol{K}, 0, 0] = I(M; Y_E^n)[\Phi_n, \boldsymbol{K}, \boldsymbol{H}, 0] = I(M; Y_E^n)[\Phi_n, \boldsymbol{K}, \boldsymbol{H}, \alpha^n]. \tag{27}$$

Proof. Since the first equation follows from the definition, we show the second equation. We define two random variables $Y_E^n(0) := K_E X^n$ and $Y_E^n(\alpha^n) := K_E X^n + H_E Z^n$. Due to the uniqueness condition of $Y_E^n(\alpha^n)$, for each $Y_E^n(0) = K_E X^n$, we can uniquely identify $Y_E^n(\alpha^n)$. Therefore, we have $I(M; Y_E^n(0)) \geq I(M; Y_E^n(\alpha^n))$. Conversely, since $Y_E^n(0)$ is given as a function of $Y_E^n(\alpha^n)$, Z^n, and H_E, we have the opposite inequality. □

Remark 2. *Theorem 2 discusses the unicast case. It can be trivially extended to the multicast case because we do not discuss the decoder. It can also be extended to the multiple unicast case, whose network is composed of several pairs of senders and receivers. When there are k pairs in this setting, the messages M and the scramble random numbers L have the forms* $(M_1, \ldots, M_k)$ *and* $(L_1, \ldots, L_k)$*. Thus, we can apply Theorem 2 to the multiple unicast case. The detail discussion for this extension is discussed in the paper [33].*

Remark 3. *One may consider the following type of attack when Alice sends the i-th transmission after Bob receives the* $i-1$*-th transmission. Eve changes the edge to be attacked in the i-th transmission dependently of the information that Eve obtains in the previous* $i-1$ *transmissions. Such an attack was discussed in [34]; there was no noise injection. Theorem 2 does not consider such a situation because it assumes that Eve attacks the same edges for each transmission. However, Theorem 2 can be applied to this kind of attack in the following way. That is, we find that Eve's information with noise injection can be simulated by Eve's information without noise injection even when the attacked edges are changed in the above way.*

To see this reduction, we consider m transmissions over the network given by the direct graph (V, E)*. We define the big graph* (V_m, E_m)*, where* $V_m := \{(v, i)\}_{v \in V, 1 \leq i \leq m}$ *and* $E_m := \{(e, i)\}_{e \in E, 1 \leq i \leq m}$ *and* (v, i) *and* (e, i) *express the vertex v and the edge e on the i-th transmission, respectively. Then, we can apply Theorem 2 with* $n = 1$ *to the network given by the directed graph* (V_m, E_m) *when the attacked edges are changed in the above way. Hence, we obtain the above reduction statement under the uniqueness condition for the network decided by the directed graph* (V_m, E_m)*.*

3.5. Application to Network Model in Section 2.6

We consider how to apply the multiple transmission setting with sequential transmission with $n = 2$ to the network given in Section 2.6; i.e., we discuss the network given in Figures 1 and 2 over the field $\mathbb{F}_q$ with $n = 2$. Then, we analyze the secrecy by applying Theorem 2.

Assume that Eve eavesdrops edges $e(2), e(5), e(6), e(7), e(8)$ and contaminates edges $e(2), e(5)$ as Figure 1. Then, we set the function τ_E from $\{1, \ldots, 11\} \times \{1, 2\}$ to $\{1, \ldots, 22\}$ as

$$\tau_E(i, l) = i + 11(l - 1). \tag{28}$$

Under the choice of η given in (14), the function $\tau_{E,\eta}$ can be set in another way as

$$\tau_{E,\eta}(i, l) = i + 2(l - 1). \tag{29}$$

Since $\gamma_{\bar{\theta}}(2,1) = 7$, $\gamma_{\bar{\theta}}(5,1) = 6$, $\gamma_{\bar{\theta}}(2,2) = 18$, $\gamma_{\bar{\theta}}(5,2) = 17$, we have

$$\begin{aligned} w_{\eta,1,1} =& \{(1,1),(2,1)\},\ w_{\eta,2,1} = \{(1,1),(2,1),(3,1)\} \\ w_{\eta,1,2} =& \{(1,1),(2,1),(3,1),(4,1),(5,1),(1,2),(2,2)\} \\ w_{\eta,2,2} =& \{(1,1),(2,1),(3,1),(4,1),(5,1),(1,2),(2,2),(3,2)\}. \end{aligned}$$

However, when the function τ_E is changed as

$$\tau_E(i,l) = i + 5(l-1) \text{ for } i = 1,\dots,5 \tag{30}$$
$$\tau_E(i,l) = 5 + i + 6(l-1) \text{ for } i = 6,\dots,11, \tag{31}$$

$w_{\eta,i,l}$ has a different form as follows. Under the choice of η given in (14), while Eve can choose $\tau_{E,\eta}$ in the same way as (29), since $\gamma_{\bar{\theta}}(2,1) = 12$, $\gamma_{\bar{\theta}}(5,1) = 11$, $\gamma_{\bar{\theta}}(2,2) = 18$, $\gamma_{\bar{\theta}}(5,2) = 17$, we have

$$\begin{aligned} w_{\eta,1,1} =& \{(1,1),(2,1),(1,2),(2,2)\} \\ w_{\eta,2,1} =& \{(1,1),(2,1),(3,1),(1,2),(2,2)\} \\ w_{\eta,1,2} =& \{(1,1),(2,1),(3,1),(4,1),(5,1),(1,2),(2,2)\} \\ w_{\eta,2,2} =& \{(1,1),(2,1),(3,1),(4,1),(5,1),(1,2),(2,2),(3,2)\}. \end{aligned}$$

We construct a code, in which the secrecy holds and Bob can detect the existence of the error in this case. For this aim, we consider two cases: (i) there exists an element $\kappa \in \mathbb{F}_q$ to satisfy the equation $\kappa^2 = \kappa + 1$; (ii) no element $\kappa \in \mathbb{F}_q$ satisfies the equation $\kappa^2 = \kappa + 1$. Our code works even with $n = 1$ in the case (i). However, it requires $n = 2$ in the case (ii). For simplicity, we give our code with $n = 2$ even in the case (i).

Assume the case (i). Alice's message is $M = (M_1, M_2) \in \mathbb{F}_q^2$, and Alice prepares scramble random numbers $L_i = (L_{i,1}, L_{i,2}) \in \mathbb{F}_q^2$ with $i = 1,2$. These variables are assumed to be subject to the uniform distribution independently. She encodes them as $X_1 = L_1$, $X_2 = L_1\kappa + L_2(1+\kappa) + M\kappa$, $X_3 = L_2 + M$, and $X_4 = L_2$. When $Z_1 = Z_2 = 0$, Bob receives

$$\begin{aligned} Y_{B,1} &= X_1 + X_2 = L_1(1+\kappa) + L_2(1+\kappa) + M\kappa, \\ Y_{B,2} &= X_1 + X_3 = L_1 + L_2 + M, \\ Y_{B,3} &= X_1 + X_4 = L_1 + L_2. \end{aligned} \tag{32}$$

Then, since $M = Y_{B,2} - Y_{B,3}$, he recovers the message by using $Y_{B,2} - Y_{B,3}$.

As shown in the following, under this code, Eve cannot obtain any information for M even though she makes active attack under the model given Figure 1. Eve's information is

$$\begin{pmatrix} Y_{E,1} \\ Y_{E,2} \\ Y_{E,3} \\ Y_{E,4} \\ Y_{E,5} \end{pmatrix} = \begin{pmatrix} \kappa & \kappa & 1+\kappa \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ \kappa & 1+\kappa & 1+\kappa \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} M \\ L_1 \\ L_2 \end{pmatrix} \tag{33}$$

when $Z_i = 0$. Proposition 2 guarantees that Eve cannot obtain any information for M when $Z_i = 0$. Thus, due to Theorem 2, the secrecy holds even when $Z_i = 0$ does not hold.

Indeed, the above attack can be considered as the following. Eve can eavesdrop all edges connected to the intermediate node $v(2)$ and contaminate all edges incoming to the intermediate node $v(2)$. The above setting means that the intermediate node $v(2)$ is partially captured by Eve. As other settings, we consider the case when Eve attacks another node $v(i)$ for $i = 1,3,4$. In this case,

we allow a slightly stronger attack; i.e., Eve can eavesdrop and contaminate all edges connected to the intermediate node $v(i)$. That is, Eve's attack is summarized as

(B1′) Eve can choose any one of nodes $v(1), \ldots, v(4)$. When $v(2)$ is chosen, she eavesdrops all edges connected to $v(2)$ and contaminates all edges incoming to $v(2)$. When $v(i)$ is chosen for $i = 1, 3, 4$, she eavesdrops and contaminates all edges connected to $v(i)$.

To apply Corollary 1 for analysis of the secrecy, we write down the low vectors $\mathbf{v}_i$ in Corollary 1 under "Vector" in Table 2. Hence, under this attack, this code has the same secrecy by the combination of Corollary 1 and Theorem 2.

Table 2. Summary of security analysis.

Node	Eavesdropping	Vector	η	Detection	Recovery
$v(1)$	$e(1)$ $e(5)$ $e(10)$	$(0,1,0)$ $(0,1,0)$ $(0,1,0)$	$\eta(1)=1$ $\eta(2)=5$ $\eta(3)=10$	$-Z_1\kappa$	$Y_{B,2}-Y_{B,3}$
$v(2)$	$e(2)$ $e(5)$ $e(6)$ $e(7)$ $e(8)$	$(\kappa,\kappa,1+\kappa)$ $(0,1,0)$ $(0,1,0)$ $(\kappa,1+\kappa,1+\kappa)$ $(0,1,0)$	$\eta(1)=5$ $\eta(2)=2$	$Z_2-Z_1\kappa$	$Y_{B,2}-Y_{B,3}$
$v(3)$	$e(3)$ $e(6)$ $e(9)$	$(1,0,1)$ $(0,1,0)$ $(1,1,1)$	$\eta(1)=3$ $\eta(2)=6$ $\eta(3)=9$	$-(Z_1+Z_2+Z_3)\kappa$	$(Y_{B,1}-Y_{B,3}(1+\kappa))\kappa^{-1}$
$v(4)$	$e(4)$ $e(8)$ $e(10)$ $e(11)$	$(0,0,1)$ $(0,1,0)$ $(0,1,0)$ $(0,1,1)$	$\eta(1)=4$ $\eta(2)=8$ $\eta(3)=10$ $\eta(4)=11$	$-Z_1-Z_2-Z_4$	$Y_{B,2}(1+\kappa)-Y_{B,1}$

Vector expresses the low vectors $\mathbf{v}_i$ of the matrix A in Corollary 1. For the case with (2), the matrix A is given in Equation (33). Detection expresses $Y_{B,1}-(Y_{B,3}+Y_{B,2}\kappa)$. If this value is not zero, Bob considers that there exists the contamination. Recovery expresses Bob's method that decodes the message M dependently of $v(i)$.

In the case (ii), we set κ as the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Then, we introduce the algebraic extension $\mathbb{F}_q[\kappa]$ of the field $\mathbb{F}_q$ by using the element e to satisfy the equation $\kappa^2 = \kappa + 1$. Then, we identify an element $(x_1, x_2) \in \mathbb{F}_q^2$ with $x_1 + x_2\kappa \in \mathbb{F}_q[\kappa]$. Hence, the multiplication of the matrix κ in $\mathbb{F}_q^2$ can be identified with the multiplication of κ in $\mathbb{F}_q[\kappa]$. The above analysis works by identifying $\mathbb{F}_q^2$ with the algebraic extension $\mathbb{F}_q[\kappa]$ in the case (ii).

3.6. Error Detection

Next, using the discussion in Section 2.2, we consider another type of security, i.e., the detectability of the existence of the error when $n = 2$ with the assumptions (B1′), (B2) and the following alternative assumption:

(B3′) The message set $\mathcal{M}$ is $\mathbb{F}_q^2$, and all information on all edges per single use are $\mathbb{F}_q$.
(B4′) The encoder on the source node can be chosen, but is restricted to linear. It is allowed to use a scramble random number, which is an element of $\mathcal{L} := \mathbb{F}_q^k$ with a certain integer k. Formally, the encoder is given as as a linear function from $\mathcal{M} \times \mathcal{L}$ to $\mathbb{F}_q^8$.

We employ the code given in Section 3.5 and consider that the contamination exists when $Y_{B,1} - (Y_{B,3} + Y_{B,2}\kappa)$ is not zero. This code satisfies the secrecy and the detectability as follows.

To consider the case with $v(2)$, we set $\eta(1) = 5, \eta(2) = 2$. Regardless of whether Eve makes contamination, $Y_{B,2} - Y_{B,3} = L_1 + L_2 + Z_1 + M - (L_1 + L_2 + Z_1) = M$. In the following, $Y_{B,i}$ for

$i = 1, 2, 3$ expresses the variable when Eve makes contamination. Hence, Bob always recovers the original message M. Therefore, this code satisfies the desired security in the case with Figure 1.

In the case of $v(3)$, we set $\eta(1) = 3, \eta(2) = 6, \eta(3) = 9$. Then, $Y_{B,1} - (Y_{B,3} + Y_{B,2}\kappa)$ is calculated through $-(Z_1 + Z_2 + Z_3)\kappa$. Hence, when $Z_1 + Z_2 + Z_3 = 0$, Bob detects no error. In this case, the contamination (Z_1, Z_2, and Z_3) does not change $Y_{B,2} - Y_{B,3}$, i.e., it does not cause any error for the decoded message. Hence, in order to detect an error in the decoded message, it is sufficient to check whether $Y_{B,1} - (Y_{B,3} + Y_{B,2}\kappa)$ is zero or not. Since $Y_{B,2} = X_1 + X_3 + Z_1 + Z_2 + Z_3$, we have $M\kappa = L_1(1+\kappa) + L_2(1+\kappa) + M\kappa - (L_1 + L_2)(1+\kappa) = Y_{B,1} - Y_{B,3}(1+\kappa)$. Hence, if Bob knows that only the edges $e(3)$, $e(6)$, and $e(9)$ are contaminated, he can recover the message by $(Y_{B,1} - Y_{B,3}(1+\kappa))\kappa^{-1}$.

In the case of $v(4)$, we set $\eta(1) = 4, \eta(2) = 8, \eta(3) = 10, \eta(4) = 11$. When $Y_{B,1} - (Y_{B,3} + Y_{B,2}\kappa) = -(Z_1 + Z_2 + Z_4) = 0$, Bob detects no error. In this case, the errors Z_1, Z_2, and Z_4 do not change $Y_{B,2} - Y_{B,3}$. Hence, it is sufficient to check whether $Y_{B,1} - (Y_{B,3} + Y_{B,2}\kappa)$ is zero or not. In addition, if Bob knows that only the edges $e(4), e(8), e(10), e(11)$ are contaminated, he can recover the message by $Y_{B,2}(1+\kappa) - Y_{B,1}$.

Similarly, in the case of $v(1)$, we set $\eta(1) = 1$, $\eta(2) = 5$, $\eta(3) = 10$. If Bob knows that only the edges $e(1), e(5), e(10)$ are contaminated, he can recover the message by the original method $Y_{B,2} - Y_{B,3}$ because it equals $L_1 + L_2 + M + Z_1 - (L_1 + L_2 + Z_1)$. In summary, when this type attack is done, Bob can detect the existence of the error. If he identifies the attacked node $v(i)$ by another method, he can recover the message.

3.7. Solution of Problem Given in Section 2.7

Next, we consider how to resolve the problem arisen in Section 2.7. That is, we discuss another type of attack given as (B1), and study the secrecy and the detectability of the existence of the error under the above-explained code with the assumptions (B2), (B3′), (B4′), and (B5).

To discuss this problem, we divide this network into two layers. The lower layer consists of the edges $e(7), e(9)$, and $e(11)$, which are connected to the sink node. The upper layer does of the remaining edges. Eve eavesdrops and contaminates any one edge among the upper layer, and eavesdrops on any one edge among the lower layer.

Again, we consider the low vectors $\mathbf{v}_i$ in Corollary 1. The vectors corresponding to the edges of the upper layer are $(0,1,0)$, $(\kappa, \kappa, 1+\kappa)$, $(1,0,1)$, and $(0,0,1)$. The vectors corresponding to the edges of the lower layer are $(\kappa, 1+\kappa, 1+\kappa)$, $(1,1,1)$, and $(0,1,1)$. Any linear combination from the upper and lower layers is not $(1,0,0)$, which implies the secrecy condition given in Corollary 1. Hence, the secrecy holds under the lower type attack. Since the contamination of this type of attack is contained in the contamination of the attack discussed in the previous subsection, the detectability also holds.

4. Conclusions

We have discussed how sequential error injection affects the information leaked to Eve when node operations are linear. To discuss this problem, we have considered the possibility that the network does not have synchronization so that the information transmission on an edges starts before the end of the the information transmission on the previous edge. Hence, Eve might contaminate the information on several edges by using the original information of these edges. Additionally, we have discussed the multiple uses of the same network when the topology and the dynamics of the network do not change and there is no correlation with the delayed information.

As a result, we have shown that there is no advantage gained by injecting an artificial noise on attacked edges. This result can be regarded as a kind of reduction theorem because the secrecy analysis with contamination can be reduced to that without contamination. Indeed, when the linearity is not imposed, there is a counterexample of this reduction theorem [21].

In addition, we have derived the matrix formulas (20) and (21) for the relation between the outputs of Alice and Bob and the inputs of Alice and Eve in the case with the multiple transmission. As the extension of Theorem 1, the similar reduction theorem (Theorem 2) holds even for the multiple

transmission. In fact, as explained in Section 3.7, this extension is essential because there exists an attack model over a network model such that the secrecy and the detectability of the error are possible with multiple uses of the same network, while it is impossible with the single use of the network. Additionally, another paper will discuss the application of these results to the asymptotic setting [33].

Indeed, there is a possibility that Eve changes H_E sequentially. This problem has been done by the paper [35] essentially using the idea of our main theorems (Theorems 1 and 2) because it refers Proposition 1 of the conference version [36], which is equivalent to our main theorems. This fact shows the importance of our reduction theorem.

Author Contributions: Formal analysis, M.H., M.O. and G.K.; Writing—original draft, M.H.; Writing—review & editing, M.O., G.K. and N.C. All authors have read and agreed to the published version of the manuscript.

Funding: This works was supported in part by the Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (B): 16KT0017, the Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (A): 17H01280, the Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (C): 16K00014, the Kayamori Foundation of Informational Science Advancement: K27-XX-467, the Okawa Research Grant: 15-02, Guangdong Provincial Key Laboratory: 2019B121203002, the Japan Society of the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (C): 17K05591.

Acknowledgments: M.H. and N.C. are very grateful to Wangmei Guo and Seunghoan Song for helpful discussions and comments.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; nor in the decision to publish the results.

References

1. Cai, N.; Yeung, R. Secure network coding. In Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT 2002), Lausanne, Switzerland, 30 June–5 July 2002; p. 323.
2. Bennett, C.H.; Brassard, G.; Crépeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inform. Theory* **1995**, *41*, 1915–1923. [CrossRef]
3. Håstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. A Pseudorandom Generator from any One-way Function. *SIAM J. Comput.* **1999**, *28*, 1364. [CrossRef]
4. Hayashi, M. Exponential decreasing rate of leaked information in universal random privacy amplification. *IEEE Trans. Inform. Theory* **2011**, *57*, 3989–4001. [CrossRef]
5. Matsumoto, R.; Hayashi, M. Secure Multiplex Network Coding. In Proceedings of the 2011 International Symposium on Networking Coding, Beijing, China, 25–27 July 2011. [CrossRef]
6. Matsumoto, R.; Hayashi, M. Universal Secure Multiplex Network Coding with Dependent and Non-Uniform Messages. *IEEE Trans. Inform. Theory* **2017**, *63*, 3773–3782. [CrossRef]
7. Kurihara, J.; Matsumoto, R.; Uyematsu, T. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans. Inform. Theory* **2013**, *61*, 3912–3936. [CrossRef]
8. Yeung, R.W.; Cai, N. Network error correction, Part I: Basic concepts and upper bounds. *Commun. Inf. Syst.* **2006**, *6*, 19–36.
9. Cai, N.; Yeung, R.W. Network error correction, Part II: Lower bounds. *Commun. Inf. Syst.* **2006**, *6*, 37–54.
10. Ho, T.; Leong, B.; Koetter, R.; Médard, M.; Effros, M.; Karger, D.R. Byzantine modification detection for multicast networks using randomized network coding. In Proceedings of the 2004 IEEE International Symposium on Information Theory (ISIT 2004), Chicago, IL, USA, 27 June–2 July 2004; p. 144.
11. Jaggi, S.; Langberg, M.; Ho, T.; Effros, M. Correction of adversarial errors in networks. In Proceedings of the 2005 IEEE International Symposium on Information Theory, (ISIT 2005), Adelaide, Australia, 4–9 September 2005; pp. 1455–1459.
12. Kadhe, S.; Sprintson, A.; Zhang, Q.E.; Bakshi, M.; Jaggi, S. Reliable and secure communication over adversarial multipath networks: A survey. In Proceedings of the 10th International Conference on Information, Communications and Signal Processing (ICICS), Singapore, 2–4 December 2015.
13. Zhang, Q.; Kadhe, S.; Bakshi, M.; Jaggi, S.; Sprintson, A. Talking reliably, secretly, and efficiently: A "complete" characterization. In Proceedings of the 2015 IEEE Information Theory Workshop (ITW), Jerusalem, Israel, 26 April–1 May 2015. [CrossRef]

14. Zhang, Q.; Kadhe, S.; Bakshi, M.; Jaggi, S.; Sprintson, A. Coding against a limited-view adversary: The effect of causality and feedback. In Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 2015), Hong Kong, China, 14–19 June 2015; pp. 2530–2534.
15. Blackwell, D.; Breiman, L.; Thomasian, A.J. The capacities of certain channel classes under random coding. *Ann. Math. Stat.* **1960**, *31*, 558–567. [CrossRef]
16. Ahlswede, R. Elimination of correlation in random codes for arbitrarily varying channels. *Z. Wahrsch. Verw. Geb.* **1978**, *44*, 159–175. [CrossRef]
17. Csiszár, I.; Narayan, P. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Trans. Inform. Theory* **1988**, *34*, 181–193. [CrossRef]
18. Dey, B.K.; Jaggi, S.; Langberg, M. Sufficiently Myopic Adversaries are Blind. *IEEE Trans. Inf. Theory* **2019**, *65*, 5718–5736. [CrossRef]
19. Tian, P.; Jaggi, S.; Bakshi, M.; Kosut, O. Arbitrarily Varying Networks: Capacity-achieving Computationally Efficient Codes. In Proceedings of the 2016 IEEE International Symposium on Information Theory, Barcelona, Spain, 10–15 July 2016.
20. Yao, H.; Silva, D.; Jaggi, S.; Langberg, M. Network Codes Resilient to Jamming and Eavesdropping. *IEEE/ACM Trans. Netw.* **2014**, *22*, 1978–1987. [CrossRef]
21. Hayashi, M.; Cai, N. Secure network code over one-hop relay network. *arXiv* **2020**, arXiv:2003.12223.
22. Jaggi, S.; Langberg, M.; Katti, S.; Ho, T.; Katabi, D.; Medard, M. Resilient network coding in the presence of Byzantine adversaries. In Proceedings of the IEEE INFOCOM 2007, Anchorage, AK, 6–12 May 2007; pp. 616–624. [CrossRef]
23. Jaggi, S.; Langberg, M.; Katti, S.; Ho, T.; Katabi, D.; Medard, M.; Effros, M. Resilient Network Coding in the Presence of Byzantine Adversaries. *IEEE Trans. Inform. Theory* **2008**, *54*, 2596–2603. [CrossRef]
24. Jaggi, S.; Langberg, M. Resilient network codes in the presence of eavesdropping Byzantine adversaries. In Proceedings of the 2007 IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, 24–29 June 2007; pp. 541–545. [CrossRef]
25. Chan, T.; Grant, A. Capacity bounds for secure network coding. In Proceedings of the Australian Communication Theory Workshop, Christchurch, New Zealand, 30 January–1 February 2008; pp. 95–100.
26. Rouayheb, S.E.; Soljanin, E.; Sprintson, A. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory* **2012**, *58*, 1361–1371. [CrossRef]
27. Ngai, C.-K.; Yeung, R.W.; Zhang, Z. Network generalized hamming weight. In Proceedings of the Workshop on Network Coding, Theory, and Applications, Lausanne, Switzerland, 15–16 June 2009; pp. 48–53.
28. Cai, N.; Yeung, R.W. Secure Network Coding on a Wiretap Network. *IEEE Trans. Inform. Theory* **2011**, *57*, 424–435. [CrossRef]
29. Cai, N.; Chan, T. Theory of Secure Network Coding. *Proc. IEEE* **2011**, *99*, 421–437.
30. Ahlswede, R.; Cai, N.; Li, S.-Y.R.; Yeung, R.W. Network information flow. *IEEE Trans. Inform. Theory* **2000**, *46*, 1204–1216. [CrossRef]
31. Yeung, R.W.; Li, S.-Y.R.; Cai, N.; Zhang, Z. *Network Coding Theory*; Now Publishers Inc.: Breda, The Netherlands, 2005.
32. Koetter, R.; Médard, M. An Algebraic Approach to Network Coding. *IEEE/ACM Trans. Netw.* **2003**, *11*, 782–795. [CrossRef]
33. Hayashi, M.; Cai, N. Asymptotically Secure Network Code for Active Attacks and its Application to Network Quantum Key Distribution. *arXiv* **2020**, arXiv:2003.12225.
34. Shioji, E.; Matsumoto, R.; Uyematsu, T. Vulnerability of MRD-Code-based Universal Secure Network Coding against Stronger Eavesdroppers. *IEICE Trans. Fundam.* **2010**, *E93-A*, 2026–2033. [CrossRef]
35. Cai, N.; Hayashi, M. Secure Network Code for Adaptive and Active Attacks with No-Randomness in Intermediate Nodes. *IEEE Trans. Inform. Theory* **2020**, *66*, 1428–1448. [CrossRef]
36. Hayashi, M.; Owari, M.; Kato, G.; Cai, N. Secrecy and Robustness for Active Attack in Secure Network Coding. In Proceedings of the IEEE International Symposium on Information Theory (ISIT 2017), Aachen, Germany, 25–30 June 2017; pp. 1172–1177.