IEEE Transactions on Quantum Engineering

Received 24 May 2023; revised 24 July 2023; accepted 16 August 2023; date of publication 28 August 2023; date of current version 13 November 2023.

Digital Object Identifier 10.1109/TQE.2023.3309590

Advantage of the Key Relay Protocol Over Secure Network Coding

GO KATO[1], MIKIO FUJIWARA[1], AND TOYOHIRO TSURUMARU[2]

[1]National Institute of Information and Communications Technology (NICT), Tokyo 184-8795, Japan
[2]Mitsubishi Electric Corporation, Information Technology R&D Center, Kanagawa 247-8501, Japan

Corresponding author: Go Kato (e-mail: go.karto.314@gmail.com)

The work of Go Kato was supported in part by the Japan Society for the Promotion of Science Kakenhi (C) under Grant 20K03779 and Grant 21K03388 and by JST CREST Grant Number JPMJCR2113, Japan. The work of Mikio Fujiwara and Toyohiro Tsurumaru was supported in part by the Ministry of Internal Affairs and Communications, Japan. ICT Priority Technology Research and Development Project under Grant JPMI00316.

ABSTRACT The key relay protocol (KRP) plays an important role in improving the performance and the security of quantum key distribution networks. On the other hand, there is also an existing research field called secure network coding (SNC), which has similar goal and structure. In this article, we analyze differences and similarities between KRPs in general and key relay using SNC schemes (KRPs-by-SNC) rigorously. We found, rather surprisingly, that there is a definite gap in security between KRPs in general and KRPs-by-SNC; that is, certain KRPs achieve better security than any SNC schemes on the same graph. We also found that this gap can be closed if we generalize the notion of SNC by adding authenticated public channels; that is, KRPs are equivalent to KRPs-by-SNC schemes augmented with authenticated public channels.

INDEX TERMS Communication networks, network coding, quantum key distribution.

I. INTRODUCTION

A quantum key distribution (QKD) link realizes distribution of secret keys to players at distant locations (see, e.g., [1] and [2]). However, the key distribution length achievable by a single QKD link is limited by the technological level of quantum optics [2]. The key relay protocol (KRP) plays an important role in improving the performance and the security of QKD networks [3], [4], [5], [6] for an expanding service area. KRPs are used to enable key distribution beyond such limitation of a single QKD link. The basic idea of the KRP is to pass a secret key of one QKD link on to another QKD link with the help of insecure public channels, such as the internet (cf., Figs. 2 and 3). The simplest type of KRPs are those using trusted nodes only, and they have been used in several QKD testbeds in the world [7], [8], [9], [10]. In Japan, Tokyo, the QKD Network has operated since 2010, and secure data transfer, storage, and secondary use have been demonstrated. Such KRPs, based on trusted nodes, are standardized in ITU-T [6]. In order to improve the convenience of QKD networks further, it is important to research and develop secure and efficient KRPs. To this end, some articles proposed improved schemes by reinterpreting the KRP as a secure data relay technique over nodes. In particular, KRPs using secure network coding (SNC) indeed turned out useful (see, e.g., [11] and [12]).

We note that KRPs as well as our results in the following can also be applied to networks of any information theoretically secure key sources, besides QKD. For example, they can be applied to key sources utilizing physical layer security [13].

The goal of this article is to rigorously analyze if there is a difference between such KRPs using SNC (henceforth, KRPs-by-SNC) and KRPs in general. This question is important for the following reason. The KRP and SNC are similar in many aspects. SNC has been studied in much greater depth than the KRP. If the KRP and SNC were not only similar but equivalent, there would be no need to study the KRP, because one could simply import the vast results of SNC into the KRP.

This question can be elaborated as follows. The KRP has similarities and differences with SNC (see Table 1). Namely, while they share the same goal of sharing secret messages, they differ in the following.

1) Public channels are available in KRPs, but not in SNC schemes.
2) KRPs use QKD links (or more generally, local key sources), while SNC schemes use secret channels.
3) In KRPs senders' role is to send secret keys, which are random bits, while in SNC schemes, they can freely choose their messages.

TABLE 1 **Similarities and Differences Between the KRP, the Conventional SNC, SNC With Public Channels, and KRP-by-SNC**

	Key relay protocol (KRP)	Secure network coding (SNC) without public channels (Conventional SNC)	SNC with public channels	KRP-by-SNC
Public channels	✓		✓	
Local key sources (e.g., QKD links)	✓			
Secret channels		✓	✓	✓
Goal	Each sender-receiver pair (or each user pair) i share a secret message			
Content of the message	Random bit k_i	Message m_i chosen by the sender	Message m_i chosen by the sender	Random bit k_i

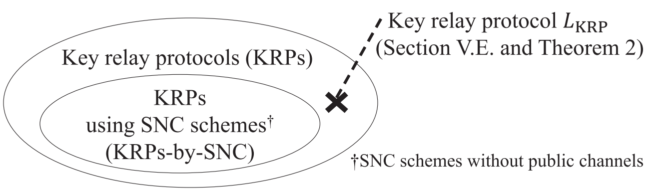

FIG. 1. **Inclusion relation of KRPs in general, and KRPs based on SNC schemes (KRPs-by-SNC). In this article, SNC schemes refer to those without public channels unless otherwise stated. The settings and the goals of KRP-by-SNC and the KRP are summarized in Table 1. The security of KRPs in general is better than that of KRPs-by-SNC (see Theorem 2).**

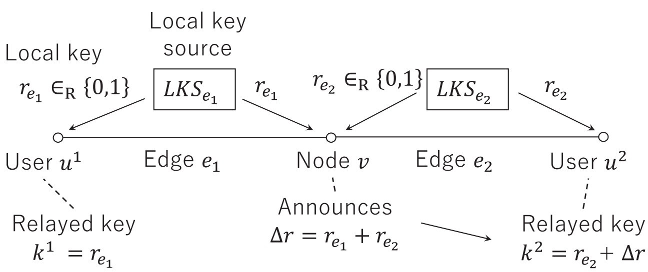

FIG. 2. **Simplest example of the KRP. On each edge e_i, there is a local key source LKS_{e_i}, which distributes a random bit $r_{e_i} \in_{\mathrm{R}} \{0, 1\}$ to both ends. Each node can also use public channels freely. User pair u^1, u^2 wishes to share a relayed key $k = (k^1, k^2)$. To this end, the midpoint v announces $\Delta r = r_{e_1} + r_{e_2}$, and then, user u^1 and u^2 each calculate $k^1 = r_{e_1}$ and $k^2 = r_{e_2} + \Delta r$.**

Here, it is straightforward to see that an SNC scheme can always be converted to a KPR-by-SNC, by restricting the messages of the SNC scheme to random keys. The nontrivial question naturally is whether KRPs-by-SNC thus obtained exhaust all KRPs in general. In other words, is it possible to convert KRP in general to a KRPs-by-SNC? This is the main question of this article. For the sake of simplicity, we will limit ourselves to the one-shot scenario.

The outline of our results is shown in Fig. 1 (or for more detail see Fig. 8). If we generalize SNC [11] schemes by adding public channels (see the third column of Table 1), then KRPs and the corresponding KRPs-by-SNC (with public channels) on the same graph are always equivalent (see Theorem 1). On the other hand, if we do not generalize SNC and limit ourselves to its conventional form (without public channels; see the second column of Table 1), then there is a definite gap in security between the KRP and SNC: on some graphs a KRP achieves better security than any conventional KRPs-by-SNC (see Theorem 2 and Corollary 1). Hence, the accumulation of past research on the conventional SNC is not sufficient to explore the potential of KRPs. This suggests that the KRP is a new research field. In other words, clarifying the relationship between KRPs-by-SNC and KRPs in general is extremely useful in clarifying the security and efficiency bounds of key relay.

II. KEY RELAY PROTOCOL

A. MOTIVATION AND EXAMPLES OF THE KRP

QKD distributes secret keys to two separate players. However, the communication distance achievable by a single set of QKD devices, or a *QKD link*, is limited by the technological level of quantum optics, and is currently in the order of 100 km [2]. For this reason, in this article, we refer to a QKD link also as a *local key source*.

There is of course a strong demand to distribute secret keys globally, or beyond the reach of a single QKD link. The KRP [3], [4], [5] aims to fulfill this demand by connecting multiple QKD links, and also by using insecure public channels, such as the internet.

Fig. 2 illustrates the simplest example of such KRPs. Users u^1 and u^2 are separated by twice the reach of a local key source, and are connected by two local key sources LKS_{e_1} and LKS_{e_2}. From these local key sources, users u^1 and u^2 receive distinct local keys $r_{e_1}, r_{e_2} \in_{\mathrm{R}} \{0, 1\}$, respectively. Then, in order for both u^1 and u^2 to share the same key $k^1 = k^2$, which we call the *relayed key*, they execute the following procedure with the help of the midpoint v.

1) The midpoint v announces the difference of the two local keys, $\Delta r = r_{e_1} + r_{e_2}$.
2) Users u^1 and u^2 calculate the relayed keys $k^1 = r_{e_1}$ and $k^2 = r_{e_2} + \Delta r$, respectively.

Note that $k^1 = k^2$ is indeed satisfied. Note also that k_i remains secret even if the announcement Δr is revealed.

This idea can be generalized to more complex network configurations. For example, one can improve the distance by serially extending the aforementioned construction [see Fig. 3(a)], or can improve the security by extending it in

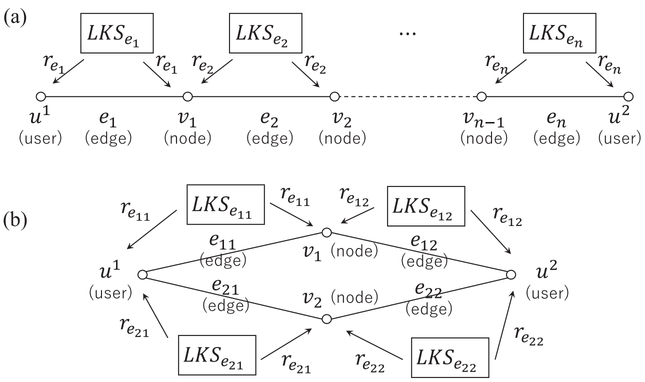

FIG. 3. **Somewhat complex examples of the KRP. (a) Serialization of Fig. 2. Nodes v_i each announce $\Delta r_i = r_{e_i} + r_{e_{i+1}}$, and then, users u^1 and u^2 calculate relayed keys $k^1 = r_{e_1}$ and $k^2 = r_{e_n} + \sum_{i=1}^{n-1} \Delta r_i$, respectively. (b) Parallelization of Fig. 2. Nodes v_i each announce $\Delta r_i = r_{e_{i1}} + r_{e_{i2}}$, and then, users u^1, u^2 each calculate $k^1 = r_{e_{11}} + r_{e_{21}}$, $k^2 = \sum_{i=1,2}(r_{e_{2i}} + \Delta r_i)$. Note that the relayed key $k = (k^1, k^2)$ remains secret here even if someone takes over an edge set $E_i = \{e_{i1}, e_{i2}\}$ ($i = 1$ or 2) and leaks local keys $r_{e_{i1}}, r_{e_{i2}}$. In this sense, we regard this construction more secure than that of Fig. 2.**

parallel [see Fig. 3(b)]. In Section II-B, we will give a formal definition of KRPs, applicable to an arbitrary network configuration.

B. FORMAL DEFINITION OF THE KRP

The outline is as follows: on an undirected graph $G = (V, E)$, pairs of users wish to share a relayed key with the help of other players on nodes V having access to local key sources and a public channels, without disseminating the message to the adversary.

1) SETTING

An undirected graph $G = (V, E)$ consists of a node set V and an edge set E. For the sake of simplicity, we assume that G is connected. Each node $v \in V$ has an individual player (denoted by the same symbol as the node), some of which constitute n_{pair} pairs of users $u_i = (u_i^1, u_i^2)$ with $i = 1, \ldots, n_{\mathrm{pair}}$. There is also an adversary, who can wiretap some edges $\subset E$.

Each edge $e \in E$ has a local key source LKS_e and a public channel PC_e, which behave as follows.

Definition 1 (Local Key Sources and Public Channels): LKS_e and PC_e operate as follows.

1) Local key source LKS_e [see Fig. 4(a)]: On input "start" command from an end node v or w, it sends a local key or a uniformly random bit $r_e \in_{\mathrm{R}} \{0, 1\}$ to both v and w. When edge e is wiretapped, it also sends r_e to the eavesdropper.
2) Public channel PC_e [see Fig. 4(b)]: On input a bit string $p_e \in \{0, 1\}^*$ from an end node, it sends p_e to the other end node and to the adversary.

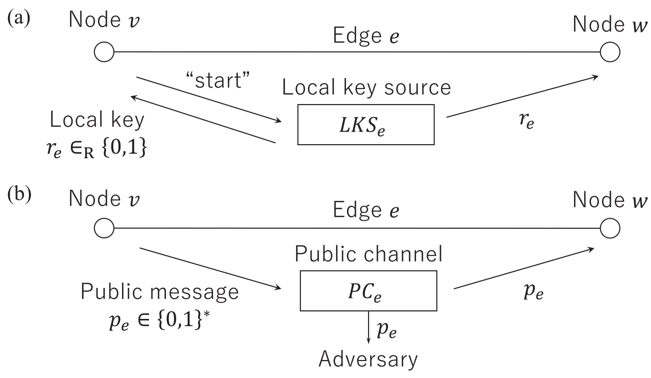

FIG. 4. **(a) Behavior of local key source LKS_e in the absence of the adversary, on edge e having end nodes v, w. (b) Public channel PC_e on the same edge.**

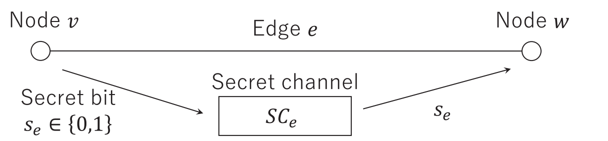

FIG. 5. **Behavior of secret channel SC_e in the absence of the adversary.**

2) KEY RELAY PROTOCOL

With the aforementioned setting, each user pair $u_i = (u_i^1, u_i^2)$ wishes to share a relayed key $k_i = (k_i^1, k_i^2)$ with the help of players V, without disseminating k_i to the adversary. To this end, they request all nodes V to execute a procedure of the following type.

Definition 2: A protocol L of the following type, performed by players V, is called a KRP.

1) All players V communicate using public channels PC_e and local key sources LKS_e.[1] Here, each LKS_e can only be used once, while PC_e can be used arbitrarily many times.
2) Each user u_i^j calculates a relayed key k_i^j.

3) SECURITY CRITERIA

There is a known collection $\mathcal{E}^{\mathrm{adv}} = \{E_1^{\mathrm{adv}}, E_2^{\mathrm{adv}}, \ldots\}$ of edge set $E_i^{\mathrm{adv}} \subset E$, which the adversary can wiretap. In each round of the protocol, the adversary chooses $E_l^{\mathrm{adv}} \in \mathcal{E}^{\mathrm{adv}}$ and wiretaps edges $e \in E_l^{\mathrm{adv}}$.

Definition 3 (Security of the KRP): A KRP L is secure against $\mathcal{E}^{\mathrm{adv}}$, if it satisfies the following.

1) Soundness: The relayed keys k_i^1, k_i^2 generated by user pair $u_i = (u_i^1, u_i^2)$ are equal and uniformly distributed, i.e., $\Pr[K_i^1 = K_i^2] = 1$, and $\Pr[K_i^j = 0] = \Pr[K_i^j = 1] = 1/2$. Also, k_i^j generated by different user pairs are independent.

[1] More precisely, the outputs (p_e, r_e, or "start") of players V are defined as functions of previously received data ($\subset \{p_e, r_e | e \in E\}$) and of random variables generated by the player. Each player sends out the outputs whenever necessary data are all received.

2) Secrecy: The relayed key pairs $k_i = (k_i^1, k_i^2)$ are unknown to the adversary even when any edge set $E_l^{\rm adv} \in \mathcal{E}^{\rm adv}$ is wiretapped. That is, for any l, we have

$$I(K_1, K_2, \ldots, K_{n_{\rm pair}}; A(E_l^{\rm adv})) = 0 \qquad (1)$$

where $A(E_l^{\rm adv})$ denotes the information that the adversary obtains by eavesdropping on edge set $E_l^{\rm adv}$.

Note that following the standard notation of information theory, throughout this article, we write actual values in a lowercase alphabet, and the corresponding random variables in the uppercase of the same alphabet. For example, the random variable corresponding to the value k_i^j is represented by K_i^j.

$A(E_l^{\rm adv})$ appearing in Definition 3 consists of local keys r_e on edges $e \in E_l^{\rm adv}$, and of all public information p_e ($e \in E$).

C. NOTES ON KRPS USED IN PRACTICAL QKD NETWORKS

In fact, the KRP defined previously is slightly different from those used in actual QKD networks. In the following, we elaborate on their relation.

1) EDGE ADVERSARY MODEL VERSUS NODE ADVERSARY MODEL

In the aforementioned definition, we employed the edge adversary model (where the adversary eavesdrops on some edges), while in actual QKD networks, the node adversary model (where the adversary can eavesdrop on information that goes in and out of a certain edges set) is usually assumed. This is not really a limitation, since the former model incorporates the latter: the situation where "the adversary eavesdrop on a node v" in the node adversary model can always be described as "all edges surrounding v are wiretapped" in the edge adversary model.

2) PASSIVE ADVERSARY VERSUS ACTIVE ADVERSARY

In the aforementioned, we assumed that the adversary is passive (honest but curious), meaning that she eavesdrops on, but does not tamper with, communication. On the other hand, in QKD, one usually assumes that the adversary is active, i.e., she can both eavesdrop on and tamper with communication.

The easiest way to convince oneself of this limitation, of course, is to accept it merely as a simplification introduced at the first step of continuing research.

On the other hand, there are also ways of justifying this limitation to some extent. That is, if the adversary is active, the following two problems arise.

1) Problem with soundness: The relayed keys may not match, $\Pr[k_i^1 \neq k_i^2] > 0$.
2) Problem with secrecy: Players V may malfunction and leak extra information to the adversary, damaging the secrecy.

But, in practical QKD networks, there are ways to solve or work around both these problems.

a) How to work around the problem with soundness: The basic idea here is the following. The relayed keys $k_i = (k_i^1, k_i^2)$ are random bits and are not meaningful by themselves, and thus, can be discarded at any time. Hence, even if the event $k_i^1 \neq k_i^2$ occurs, players can discard k_i^1, k_i^2 and repeat new rounds the KRP (including QKD as local key sources) until they obtain k_i^1, k_i^2 satisfying $k_i^1 = k_i^2$. This can generally decrease the key generation speed, but the secrecy remains intact.

Of course, in order for the aforementioned idea to actually function in practice, user pairs u_i must be able to detect an error (check if $k_i^1 = k_i^2$ or not) with a sufficiently small failure probability. This is also realizable by using information theoretically secure message authentication codes (see, e.g., [14, Sec. 4.6]).

Combining these ideas, we obtain the following method.

a) User pairs $u_i = (u_i^1, u_i^2)$ repeat a KRP n times and share n-bit relayed keys $\vec{k}_i^1, \vec{k}_i^2 \in \{0, 1\}^n$.
b) User u_i^1 calculates the hash value $\sigma_i = h(\vec{k}_i^1)$ of $\vec{k}_i^1$ using an ε-difference universal hash function h [14]. User u_i^1 then encrypts σ_i by the one-time pad (OTP) scheme (see, e.g., [14]) and sends it to u_i^2. (In fact, this entire step corresponds to authenticating message $\vec{k}_i^1$ using [14, Construction 4.24].)
c) User u_i^2 decrypts the received ciphertext to obtain σ_i. If $\sigma_i \neq h(\vec{k}_i^2)$, u_i^2 announces that the relayed keys $\vec{k}_i^1$ and $\vec{k}_i^2$ must be discarded. (Here, u_i^2 authenticates his announcement by again using Construction 4.24 of [14].)

In this method, steps 2 and 3 each consume a preshared key[2] of a length proportional to $|\sigma_i|$, the length of σ_i. However, one can set $|\sigma_i|$ negligibly small compared with n, with an appropriate choice of the function h and for sufficiently large n. Thus, the net relayed key obtained by this method almost equals n. For example, by using a polynomial-based ε-difference universal hash function, we have $|\sigma_i| = O(\varepsilon^{-1} \log n)$ with ε being the failure probability of the error detection.

b) Countermeasure against problem with secrecy: As for the problem with secrecy, one countermeasure is to restrict ourselves with *linear* KRPs.

Here, a linear KRP means the one where players V are *linear*. A player $v \in V$ being linear means that its outputs p_e and r_e are all linear functions of previously received data ($\subset \{p_e, r_e | e \in E\}$) and of random variables generated by the

[2]The security proofs of QKD require that its public communication be authenticated. A customary way to fulfill this requirement in practical QKD systems is that each user pair always keeps sharing a relatively small amount of the secret key (preshared key), and uses it to authenticate their public communication, e.g., by the methods given in [14, Sec. 4.6] and [15]. Here, we use those preshared keys also for KRPs.

player. In such restricted case, we can prove the following lemma.

Lemma 1: If a linear KRP is secure against passive (i.e., honest but curious) adversaries, it is also secure against active adversaries.

This lemma is a variant of Theorem 1 in [16], which was previously obtained for the SNC. As the proof is essentially the same as in [16], we here only give a sketch.

Suppose, for example, that the active adversary modifies a local key $r_{e'}$ to $r_{e'} + \Delta r$, which is to be input to a node v. With v being linear, v's subsequent outputs all change linearly in Δr; for example, a public message p_e, which v outputs, changes to $p_e + f(\Delta r)$ with f being a linear function. Since those linear responses to tampering, such as $f(\Delta r)$, are all predictable, we can conclude that the adversary gains nothing by tampering with communication.

Of course, this countermeasure is not applicable when one must use nonlinear KRPs. Such cases must be considered separately. In this respect, the existing literature on network codes resilient against active attackers, e.g., [17], would be helpful.

III. MAIN RESULTS: RELATION BETWEEN THE KRP AND SNC

As readers familiar with SNC (see, e.g., [11] and [12]) may have already noticed, the KRP defined in the previous section has similarities and differences with SNC (see Table 1). That is, while they both share the same goal that each sender–receiver pair (or each user pair) share a secret message, they differ in the following.

1) Public channels PC_e are used in the KRP, but not in SNC.
2) The KRP uses local key sources LKS_e, while SNC uses secret channels.
3) In SNC, the sender can choose the message freely. However, in the KRP, the message (which we called the relayed key k_i in the previous section) must be uniformly random, and thus, the sender does not have freedom to choose it.

From this observation, the question naturally arises whether these differences are really essential. For example, is it not possible that there is actually a way of converting KRPs to SNC schemes, and that they are shown to be equivalent? In this section, we answer this question. The outline of our results is as follows.

First, if we eliminate the aforementioned difference 1) by hand, that is, if we generalize SNC [11] by adding public channels, then we can simultaneously resolve the remaining differences, 2), and 3), as well. As a result of this, we can show that the generalized form of SNC (i.e., SNC with public channels, in the third column of Table 1) and the KRP are equivalent (see Theorem 1).

On the other hand, if we do not generalize SNC and limit ourselves with its conventional form (the second column of Table 1), then there is a definite gap in security between SNC and the KRP: there are situations where KRPs achieve better securities than the conventional SNC schemes, without public channels (see Theorem 2).

A. DEFINITION OF SNC WITH PUBLIC CHANNELS

We begin with a formal definition of SNC with public channels, which is mentioned previously and corresponds to the third column of Table 1.

The conventional SNC (the second column of Table 1) is the special case of this scheme where the use of public channels is prohibited.

1) Setting

The setting is the same as that of the KRP, given in Section II-B1, except the following.

1) Of each user pair $u_i = (u_i^1, u_i^2)$, one user (e.g., u_i^1) is named the sender a_i, and the other (e.g., u_i^2) the receiver b_i. Thus, either $(u_i^1, u_i^2) = (a_i, b_i)$ or $(u_i^1, u_i^2) = (b_i, a_i)$ holds.
   This nonidentical correspondence is necessary because, in SNC, messages are not a random bit (as in the KRP), but must be chosen by the sender a_i; see Definition 5.
2) Local key sources LKS_e are replaced by the secret channels SC_e, defined in Definition 4 as follows.

Definition 4 (Secret Channels): On input a bit $s_e \in \{0, 1\}$ from one end node, secret channel SC_e sends s_e to the other end node; see Fig. 5. When edge e is wiretapped, it also sends s_e to the eavesdropper.

In comparison with the conventional SNC [11], the aforementioned setting differs only in that players V can use public channels PC_e in addition to secret channels SC_e (see Table 1).

2) SNC With Public Channels

The goal of our SNC with public channels is the same as that of the conventional SNC [11]. Each sender–receiver pair (a_i, b_i) wishes to exchange message m_i with the help of other players on nodes V, without disseminating m_i to the adversary.

Definition 5 (SNC With Public Channels): We call a protocol of the following type a SNC scheme with public channels.

1) Each sender a_i chooses a message $m_i \in \{0, 1\}$ aimed at the receiver b_i.
2) Players V communicate by using public channels PC_e and secret channels SC_e.[3] Here, each SC_e can only be used once, while PC_e can be used arbitrarily many times.
3) Each receiver b_i calculates message $\hat{m}_i \in \{0, 1\}$.

In comparison with Definition 2 for the KRP, the aforementioned Definition 5 differs only in that LKS_e are replaced

[3] As in the case of the KRP, we assume that the outputs (p_e, s_e) of players are defined as functions of previously received data $(\subset \{p_e, s_e | e \in E\})$ and of random variables generated by the player. We also assume that each player sends out the output whenever necessary data are all received.

by SC_e, and that senders a_i can arbitrarily choose message m_i, which need not be uniformly distributed, unlike the relayed key k_i^1 (cf., Table 1).

3) Security Criteria

The security criteria is essentially the same as Definition 3 for the case of the KRP. That is, there is again a known collection $\mathcal{E}^{\rm adv} = \{E_1^{\rm adv}, E_2^{\rm adv}, \dots\}$ of wiretap sets $E_l^{\rm adv} \subset E$. In each round of the SNC scheme, the adversary chooses $E_l^{\rm adv} \in \mathcal{E}^{\rm adv}$ and wiretap edges $e \in E_l^{\rm adv}$.

Definition 6 (Security of SNC With Public Channels): An SNC scheme L is secure against $\mathcal{E}^{\rm adv}$, if it satisfies the following.

1) Soundness: Sender a_i's message m_i reaches receiver b_i without error; $\Pr[M_i = \hat{M}_i] = 1$.
2) Secrecy: Messages m_i and $\hat{m}_i$ are unknown to the adversary even when any edge set $E_j^{\rm adv} \in \mathcal{E}^{\rm adv}$ is wiretapped. That is, for any l, we have

$$I(M_1, M_2, \dots, M_{n_{\rm pair}}; A(E_l^{\rm adv})) = 0 \quad (2)$$

where $A(E_l^{\rm adv})$ denotes the information that the adversary obtains by eavesdropping on edges $E_l^{\rm adv}$, i.e., $A(E_l^{\rm adv})$ consists of secret bits s_e on edges $e \in E_l^{\rm adv}$, and of all public information p_e $(e \in E)$.

In comparison with Definition 3 for the KRP, the aforementioned Definition 6 differs in that m_i need not be uniformly distributed (cf., Table 1), and that local keys r_e included in the adversary's information $A(E_j^{\rm adv})$ are replaced by secret bits s_e.

B. SNC WITH PUBLIC CHANNELS AND THE KRP ARE EQUIVALENT

SNC with public channels thus defined are in fact equivalent to the KRP defined in the previous section.

Theorem 1 (Equivalence of SNC With Public Channels, and KRP): SNC schemes with public channels and KRPs can always achieve the same security as follows.

1) Given a KRP L compatible with a graph G and user configuration $u_i = (u_i^1, u_i^2)$, which is secure against wiretap sets $\mathcal{E}^{\rm adv}$, one can construct an SNC scheme with public channels L', which is compatible with the same G and u_i, and also secure against the same $\mathcal{E}^{\rm adv}$. This is true whether the sender and the receiver for each user pair u_i in L' are assigned as $(u_i^1, u_i^2) = (a_i, b_i)$ or $(u_i^1, u_i^2) = (b_i, a_i)$ (for the meaning of this notation, see Section III-A1).
2) Given an SNC scheme L (with or without public channels) compatible with a graph G and a sender–receiver configuration $u_i = (a_i, b_i)$, which is secure against $\mathcal{E}^{\rm adv}$, one can construct a KRP L' compatible with the same G and u_i, which is secure against the same $\mathcal{E}^{\rm adv}$.

Therefore, if one wishes to analyze the potential and limitations of the KRP, it is necessary and sufficient to investigate SNC with public channels.

We will prove Theorem 1 in Section IV.

C. SNC WITHOUT PUBLIC CHANNELS AND THE KRP ARE NOT EQUIVALENT

However, in order for the aforementioned Theorem 1 to hold, it was in fact essential that we generalized SNC by adding public channels. The equivalence with the KRP no longer holds if we limit ourselves with the conventional SNC, i.e., SNC schemes without public channels. More precisely, we have the following theorem.

Theorem 2 (SNC Without Public Channels (Conventional SNC) and KRP Are Not Equivalent): There exists a combination of a graph G, a user configuration u_i, and wiretap sets $\mathcal{E}^{\rm adv}$ for which there exists a secure KRP $L_{\rm KRP}$, but there exists no secure SNC scheme without public channels.

This is true whether the sender and the receiver for each user pair u_i (in the SNC without public channels) are assigned as $(u_i^1, u_i^2) = (a_i, b_i)$ or $(u_i^1, u_i^2) = (b_i, a_i)$ (for the meaning of this notation, see Section III-A1).[4]

The proof of this theorem is give in Section V.

In short, there are situations where the KRPs achieve better securities than the conventional SNC. Hence, the accumulation of past research on the conventional SNC is not sufficient to explore the potential of the KRP. In this sense, the KRP is a new research field.

Combining Theorems 1 and 2, we can also obtain the following corollary.

Corollary 1 (The Security of SNC With Public Channels ≠ The security of SNC Without Public Channels (Conventional SNC)): There exists a combination of a graph G, a user configuration u_i, and wiretap sets $\mathcal{E}^{\rm adv}$ for which there exists a secure SNC scheme with public channel, but there exists no secure SNC scheme without public channels.

IV. PROOF OF THEOREM 1

To prove item 1), note that operations of LKS_e can be simulated by using SC_e. That is, if an end node v of edge e wishes to send a local key r_e to the other end node w, it suffices that v generates a random bit $r_e \in_{\rm R} \{0, 1\}$ by itself and sends it to w via SC_e (see Fig. 6).

By applying this simulation to all LKS_e included in L, one obtains a protocol L' where user pairs $u_i = (u_i^1, u_i^2)$ share relayed key $k_i = (k_i^1, k_i^2)$ in the same setting as in SNC with the public channel, given in Section III-A1.

Then, by using k_i thus obtained to encrypt message m_i by the OTP encryption scheme [14], one obtains L'. Here, the OTP encryption scheme is the following. User u_i^1 encrypts m_i as the ciphertext $c_i = m_i + k_i^1$ and sends it to u_i^2 via public channel. Then, u_i^2 decrypts it as $\hat{m}_i = c_i + k_i^2$.

[4]It is important to note that this theorem applies even to SNC schemes on undirected graphs. If one is somehow allowed to limit oneself with SNC on directed graphs, the counterexample $L_{\rm KRP}$ can be constructed straightforwardly.

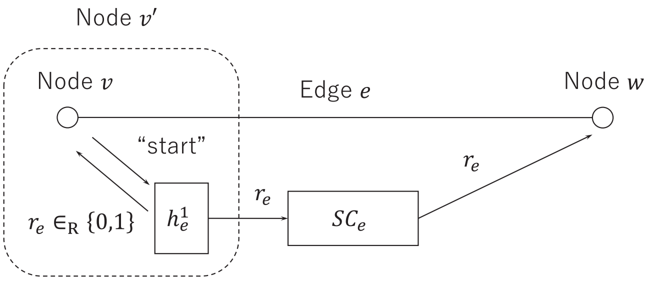

FIG. 6. Construction for simulating a local key source LKS_e (Definition 1 and Fig. 4) by using a secret channel SC_e. We add a function h_e^1 to an end node v of e (the one that would start LKS_e), and regard them as a new node v'. The function h_e^1 operates as follows: when it receives "start" command from v, it generates a uniformly random bit $r_e \in_R \{0,1\}$ and sends it to SC_e.

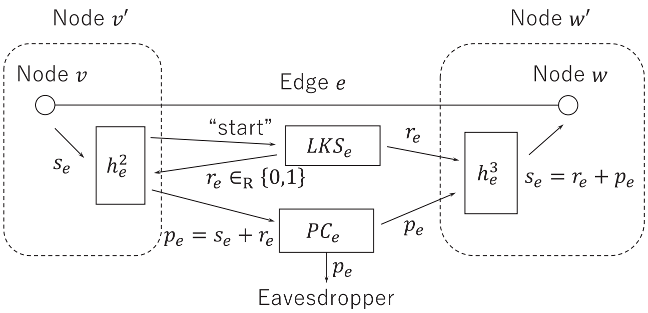

FIG. 7. Construction for simulating a secret channel SC_e [see Definition 4 and Fig. 5(a)] by using the local key source LKS_e and the public channel PC_e. We add a function h_e^2 to an end node v of e (the one that would start LKS_e), and regard them as a new node v'. Function h_e^2 has two operations, namely, on receiving s_e from v, h_e^2 sends out "start" command to LKS_e, and on receiving r_e from PC_e, h_e^2 sends out $p_e = s_e + r_e$ to PC_e. Similarly, we add a function h_e^3 to the other end node w, and regard them as a new node w'. Function h_e^3 has one operation: on receiving r_e from LKS_e and p_e from PC_e, h_e^3 sends out $s_e = r_e + p_e$ to w.

The soundness of L' is obvious from the construction. The secrecy of L' follows from that of L, since the adversary's information is the same in L and L'. Indeed, in L', the secrecy of r_e on nonwiretapped edges e is obvious by the construction, and thus, the security of k_i from that of L. Then, the secrecy of m_i follows from that of the OTP. This completes the proof of item 1 of Theorem 1.

For the proof of item 2), note that SC_e can be simulated by the local key source LKS_e and the public channel PC_e. When an end node u wishes to send a bit s_e to the other end node v, it first distributes a random bit r_e by switching on the local key source LKS_e. Then, u sends s_e to v secretly by encrypting it by the OTP encryption scheme with r_e being the secret key (see Fig. 7).

By applying this construction to all secret channels included in L, one obtains a new KRP, which we denote by L'. By construction, it is obvious that message m_i as well as the adversary's information are the same, whether in L or in L'. This completes the proof of item 2) of Theorem 1.

V. PROOF OF THEOREM 2

Theorem 2 asserts that the difference of structure between the KRP and the conventional SNC (shown in the first and the third columns of Table 1, and also explained in the first paragraph of Section III) cause a definite gap in security (see Fig. 1). In the following, we prove this theorem by proving a set of more general lemmas (see Fig. 8).

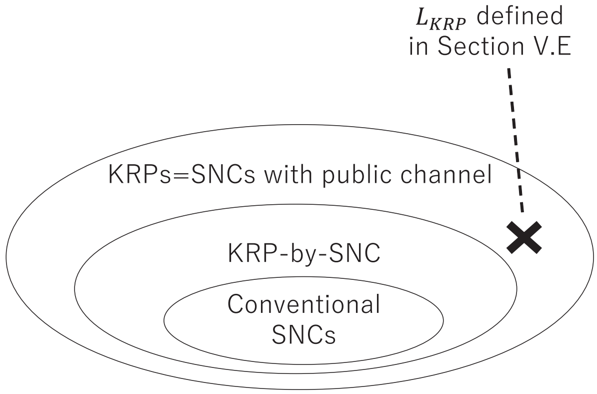

FIG. 8. Inclusion relation of SNC schemes with and without public channels, KRPs, and KRPs by using SNC without public channels (KRPs-by-SNC).

That is, we introduce another new type of protocols that we call *KRP-by-SNC* (KRP by the setting of SNC without public channels), which corresponds to the fourth column of Table 1. Then, we show that secure schemes satisfy the relations \begin{equation*}

$$\text{Conventional SNC} \subseteq \text{KRP-by-SNC} \subseteq \text{KRP}$$

(Lemmas 2 and 3), as well as

$$\text{KRP-by-SNC} \neq \text{KRP}.$$

(Lemma 4). These two relations together assert that the KRP is strictly more secure than the conventional SNC, which completes the proof of Theorem 2.

A. DEFINITION OF KRP-BY-SNC

KRP-by-SNC (KRP by the setting of SNC without public channels) is a variant of SNC corresponding to the fourth column of Table 1. That is, it uses the same setting as in the conventional SNC, where players V use the secret channels SC_e only. On the other hand, the goal is the same as in the KRP, where user pairs u_i aim to share a random bit k_i.

Alternatively, KRP-by-SNC can also be considered as a variant of KRP, obtained by replacing the public channels PC_e and the local key sources LKS_e with the secret channels SC_e.

The formal definition of KRP-by-SNC is as follows.

1) Setting

The setting is the same as that of SNC without public channels (the conventional SNC), except the following.

1) We denote user pairs by $u_i = (u_i^1, u_i^2)$, as in the case of KRP. We make no distinction between the sender and the receiver.

We use this notation to stress that our goal here is to distribute a random bit k_i, and thus, no particular user (u_i^1 or u_i^2) is entitled to choose the value k_i.

2) *KRP-by-SNC*

The goal here is the same as that of KRP. Each user pair $u_i = (u_i^1, u_i^2)$ shares a uniformly random key $k_i = (k_i^1, k_i^2)$, without disseminating it to the adversary. Thus, the basic form of the protocol should be the same as that of the KRP given in Definition 2. However, as the setting here is different (SC_e are used instead of PC_e and LKS_e), we need to modify Definition 2 as follows.

Definition 7 (KRP-by-SNC): A protocol L of the following type, performed by players V, is called a KRP-by-SNC.

1) Players V communicate by using secret channels SC_e.[5] Here, each SC_e can only be used once.
2) Each user u_i^j calculates its relayed key k_i^j.

3) *Security Criteria of KRP-by-SNC*

We use the same security criteria as in the KRP, namely, Definition 3. However, there is a caveat here: in the present case of KRP-by-SNC, the adversary's information $A(E_l^{\mathrm{adv}})$ appearing in Definition 3 consists of the secret bits s_e on wiretapped edges $e \in E_l^{\mathrm{adv}}$. This is because, in KRP-by-SNC, players V use the secret channels SC_e only.

B. PROOF OF THEOREM 2

The following two lemmas assert that the security of KRP-by-SNC is between those of SNC and KRP.

Lemma 2 (Secure Conventional SNC $\subseteq$ Secure KRP-by-SNC): KRP-by-SNCs can always achieve the same security as the conventional SNC schemes. That is, given a conventional SNC scheme L compatible with a graph G and a sender–receiver configuration $u_i = (a_i, b_i)$ that is secure against wiretap sets $\mathcal{E}^{\mathrm{adv}}$, one can construct a KRP-by-SNC L' compatible with the same G and u_i that is secure against the same $\mathcal{E}^{\mathrm{adv}}$.

Proof: KRP-by-SNC L' can be realized by letting the sender a_i of SNC L choose a random bit k_i and send it out as a message m_i. It is straightforward to verify that the security of L', defined in Section V-A2, follows from the security of L, defined in Section III-A3. □

Lemma 3 (Secure KRP-by-SNC $\subseteq$ Secure KRP): KRP can always achieve the same security as KRP-by-SNC. That is, given a KRP-by-SNC L compatible with a graph G and a user configuration u_i that is secure against wiretap sets $\mathcal{E}^{\mathrm{adv}}$, one can construct a KRP L' compatible with the same G and u_i that is secure against the same $\mathcal{E}^{\mathrm{adv}}$.

Proof: This can be proved in the same manner as in the proof of item 2) of Theorem 1. By rewriting all the secret channels SC_e appearing in KRP-by-SNC L as the OTP-encrypted channels using LKS_e and PC_e, we obtain KRP L'. □

[5]We also assume that the outputs of players are defined as functions of previously received data and of random variables generated by the player, and that each player sends out the output whenever necessary data are all received.

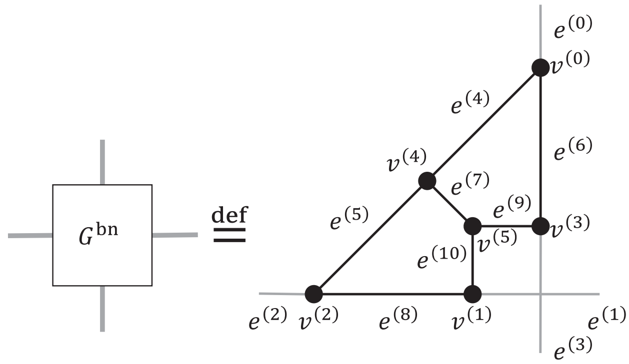

FIG. 9. Subgraph G^{bn} is defined by the black nodes and edges on the right-hand side. This subgraph G^{bn} is in fact the well-known modified butterfly network. When there are multiple copies of G^{bn}, we distinguish them as $G^{\mathrm{bn}}_{s,i}$ by indices s, i. Gray edges are the external edges that connect $G^{\mathrm{bn}}_{s,i}$ with another subgraph $G^{\mathrm{bn}}_{s',i'}$ or with a user u_i^1 or u_i^2.

According to the aforementioned Lemma 3, there still remains the possibility that the securities of KRP-by-SNC and KRP are equal. Lemma 4 as follows disproves this possibility.

Lemma 4 (Secure KRP-by-SNC $\neq$ Secure KRP): For a graph G_0, a user configuration u_i (defined in Section V-D), and the empty wiretap set $\mathcal{E}^{\mathrm{adv}} = \{\varnothing\}$, there exists a secure KRP L_{KRP} (defined in Section V-E1), but there exists no secure KRP-by-SNC.

Hence, there is a definite gap in security between KRP-by-SNC and KRP. Combined with Lemma 2, this also means that there is a definite gap in security between KRP and the conventional SNC, which completes the proof of Theorem 2.

The rest of this section is devoted to the proof of Lemma 4. The outline of the proof is as follows. First, we define a graph G_0 and a configuration of user pairs u_i (see Section V-D), as well as a KRP L_{KRP} compatible with them (see Section V-E1). Then, we show that L_{KRP} is secure against $\mathcal{E}^{\mathrm{adv},G_0} := \{\varnothing\}$, i.e., secure when no edge is wiretapped (see Section V-E2). Then, we show that there exists no secure KRP-by-SNC compatible with the same G_0 and u_i even when no edge is wiretapped (see Section V-F).

C. NOTATION

For ease of notation, we will often write r_e and p_e defined in Definition 1 as $r[e]$ and $p[e]$. Similarly, we often write s_e defined in Definition 4 as $s[e]$.

D. DESCRIPTION OF THE GRAPH G_0 AND THE USER CONFIGURATION u_i

1) *Description Using Figures*

We define the graph G_0 by a nested structure as in Figs. 9–11.

That is, we first define a subgraph G^{bn} by Fig. 9, which is in fact the well-known modified butterfly network [18]. Then,

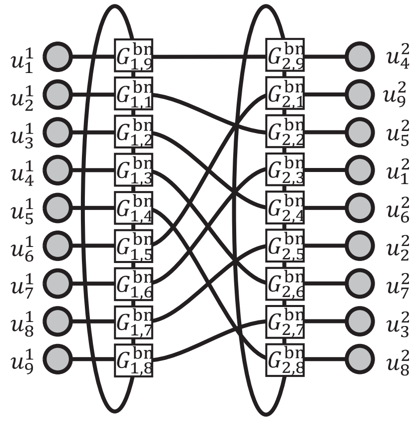

FIG. 10. **Graph G_0 and the user configuration u_i. Subgraphs $G^{\mathrm{bn}}_{s,i}$ are copies of the subgraph G^{bn} defined in Fig. 9. Edges are wired according to the rule of Fig. 11.**

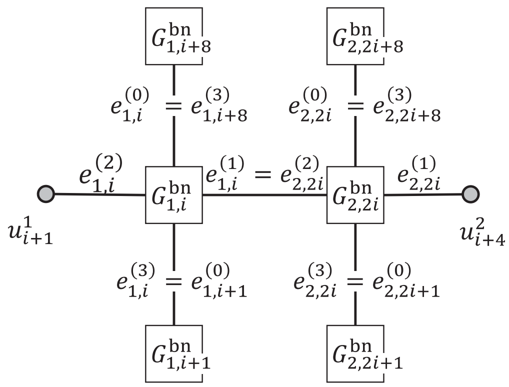

FIG. 11. **Fundamental wiring rule of the graph G_0 depicted in Fig. 10. One can reconstruct graph G_0 by repeating this rule.**

we construct the graph G_0 by connecting subgraphs[6] $G^{\mathrm{bn}}_{s,i}$ and users u^j_i, as in Figs. 10 and 11.

2) Alternative Description Using Equations

The same graph $G_0 = (V_0, E_0)$ and the user pairs $u_i = (u^1_i, u^2_i)$ can also be defined using equations, as follows.

The node set V_0 consists of the user pairs u^s_i, and of the nodes $v^{(\alpha)}_{s,i}$ composing subgraphs $G^{\mathrm{bn}}_{s,i}$, where indices s, i, and α are in the ranges $s \in \{1, 2\}$, $i \in \mathbb{Z}/9\mathbb{Z}$,[7] and $\alpha \in \{0, 1, 2, 3, 4, 5\}$. According to this notation, we identify u^s_i, $v^{(\alpha)}_{s,i}$, and $G^{\mathrm{bn}}_{s,i}$ with u^s_{i+9}, $v^{(\alpha)}_{s,i+9}$, and $G^{\mathrm{bn}}_{s,i+9}$, respectively, in the following.

The edge set E_0 consists of the internal edges of subgraphs $G^{\mathrm{bn}}_{s,i}$ as

$$\{v^{(0)}, v^{(4)}\} = e^{(4)}, \quad \{v^{(2)}, v^{(4)}\} = e^{(5)}, \quad \{v^{(0)}, v^{(3)}\} = e^{(6)}$$

$$\{v^{(4)}, v^{(5)}\} = e^{(7)}, \quad \{v^{(2)}, v^{(1)}\} = e^{(8)}, \quad \{v^{(5)}, v^{(3)}\} = e^{(9)}$$

$$\{v^{(5)}, v^{(1)}\} = e^{(10)} \tag{3}$$

edges connecting different subgraphs $G^{\mathrm{bn}}_{s,i}$

$$\{v^{(1)}_{1,i}, v^{(2)}_{2,2i}\} = e^{(1)}_{1,i} = e^{(2)}_{2,2i} \tag{4}$$

$$\{v^{(3)}_{s,i}, v^{(0)}_{s,i+1}\} = e^{(3)}_{s,i} = e^{(0)}_{s,i+1} \tag{5}$$

and edges connecting subgraphs $G^{\mathrm{bn}}_{s,i}$ and users u^s_i

$$\{u^1_{i+1}, v^{(2)}_{1,i}\} = e^{(2)}_{1,i}, \ \{v^{(1)}_{2,2i}, u^2_{i+4}\} = e^{(1)}_{2,2i} \tag{6}$$

where $s \in \{1, 2\}$, $i \in \mathbb{Z}/9\mathbb{Z}$.

3) Notation Related With $G^{\mathrm{bn}}_{s,i}$

In the following, for ease of notation, we will often suppress subscripts s and i (corresponding to one of subgraphs $G^{\mathrm{bn}}_{s,i}$), if it is clear from the context which subgraph $G^{\mathrm{bn}}_{s,i}$ we focus on. Also, whenever we say a subgraph $G^{\mathrm{bn}}_{s,i}$ is a sender/receiver, it means that a node inside $G^{\mathrm{bn}}_{s,i}$ is a sender/receiver.

E. KRP L_{KRP} COMPATIBLE WITH G_0 AND u_i

1) Construction of L_{KRP}

KRP L_{KRP} consists of the following two steps.

a) First step: The goal here is that: for all s, i and $\beta \in \{0, 2\}$, the node $v^{(\beta)}_{s,i}$ sends the local key $r[e^{(\beta)}_{s,i}]$ to the node $v^{(\beta+1)}_{s,i}$ secretly.

In order to realize this task, we use the following idea. Note that, if secret channels SC_e were available, this task could be realized by using the well-known modified butterfly network coding in each subgraph $G^{\mathrm{bn}}_{s,i}$ [18]. However, since we do not have secret channels SC_e in the present setting, we emulate them with the OTP encryption using local keys supplied by LKS_e and with public communication on PC_e (as we did in the proof of Theorem 1; also see Fig. 7). Namely, whenever a node $v^{(\alpha)}$ wishes to secretly transmit a bit r to an adjacent node $v^{(\alpha')}$, it encrypts r using the key supplied by LKS_e on the edge e between $v^{(\alpha)}$ and $v^{(\alpha')}$, and sends it to $v^{(\alpha')}$ via the public channel PC_e. In the following, we often write this emulated secret transmission as $v^{(\alpha)} \to v^{(\alpha')} : r$.

Due to this idea and notation, our first step of L_{KRP} takes the following form (see Fig. 12):

$$v^{(0)} \to v^{(3)} : r[e^{(0)}] \tag{7}$$

$$v^{(0)} \to v^{(4)} : r[e^{(0)}] \tag{8}$$

$$v^{(2)} \to v^{(1)} : r[e^{(2)}] \tag{9}$$

$$v^{(2)} \to v^{(4)} : r[e^{(2)}] \tag{10}$$

$$v^{(4)} \to v^{(5)} : r[e^{(0)}] \oplus r[e^{(2)}] \tag{11}$$

$$v^{(5)} \to v^{(1)} : r[e^{(0)}] \oplus r[e^{(2)}] \tag{12}$$

$$v^{(5)} \to v^{(3)} : r[e^{(0)}] \oplus r[e^{(2)}] \tag{13}$$

[6] Copies of the subgraph G^{bn} labeled with indices s, i.

[7] We use this notation to suggest that modulo 9 is implied in arithmetic involving variable i.

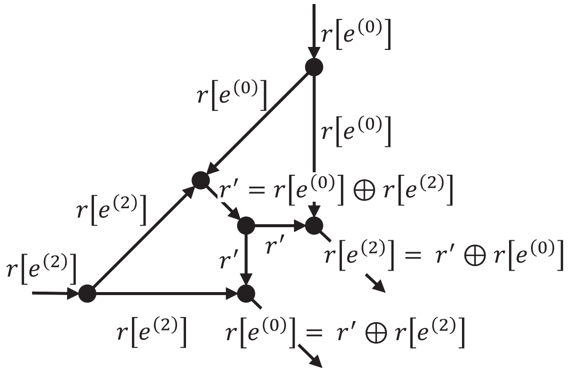

FIG. 12. First step of L_{KRP}, given in Section V-E1a. This is essentially the same as the well-known modified butterfly network coding.

and $v^{(1)}$ and $v^{(3)}$ obtain the values $(r[e^{(0)}] \oplus r[e^{(2)}]) \oplus r[e^{(2)}]$ and $(r[e^{(0)}] \oplus r[e^{(2)}]) \oplus r[e^{(0)}]$, respectively.

b) Second step: Next, using the local keys $r[e^{(\beta)}_{s,i}]$ thus obtained, each user pair $u_i = (u_i^1, u_i^2)$ shares a relayed key. They do this by performing the serial KRP of Fig. 3(a), on a straight path consisting of edges $v^{(3)}_{1,i+8}$, $v^{(1)}_{1,i}$, $v^{(3)}_{2,2i}$, and $v^{(1)}_{2,2i+1}$.

Namely, the nodes in the middle of the path announce $r[e^{(2)}_{1,i+8}] \oplus r[e^{(0)}_{1,i}]$, $r[e^{(0)}_{1,i}] \oplus r[e^{(2)}_{2,2i}]$, $r[e^{(2)}_{2,2i}] \oplus r[e^{(0)}_{2,2i+1}]$, and $r[e^{(0)}_{2,2i+1}] \oplus r[e^{(1)}_{2,2i+1}]$, and then, the user u_i^2 obtains the bit $r[e^{(2)}_{1,i+8}]$ by summing up the published bits and the local key $r[e^{(1)}_{2,2i+1}]$.

2) Security of L_{KRP}

From the aforementioned construction, we immediately have the following lemma.

Lemma 5 (Security of L_{KRP}): The KRP L_{KRP} is secure against wiretap sets $\mathcal{E}^{adv,G_0} = \{\emptyset\}$.

Proof: We give a detailed proof in Appendix. The basic idea of the proof is as follows.

The security (the secrecy and the soundness) of the emulated secret channels used in the first step is obvious by construction, and thus, the security of the local key $r[e^{(\beta)}_{s,i}]$ is guaranteed by that of the modified butterfly network coding. The security of the serial KRP is also obvious by construction. These two facts together guarantee the security of L_{KRP}. □

F. PROOF THAT THERE EXISTS NO SECURE KRP-BY-SNC COMPATIBLE WITH G_0 AND u_i

Lemma 4 asserts that there exists no secure KRP-by-SNC compatible with G_0 and u_i defined previously, even when no edge is wiretapped. In the following, we prove this assertion by first supposing that such KRP-by-SNC exists, and then, deriving a contradiction.

In order to describe the contradiction, it is convenient to number edges e according to the time when the secret channel SC_e is used. Obviously, such numbering is possible for any KRP-by-SNC. Formally, this numbering is equivalent to the following total order $\prec$.

Definition 8 (Total Order $\prec$ of Edges): Given a KRP-by-SNC L on a graph $G = (V, E)$, we write $e \prec e'$ ($e \in E$ is smaller than $e' \in E$) if the secret channel SC_e is used before $SC_{e'}$ is used in L.

Now, if we suppose that there exists a secure KRP-by-SNC L_0 (compatible with G_0, u_i, and $\mathcal{E}^{adv} = \{\emptyset\}$), L_0 must satisfy the condition of the following lemma.

Lemma 6: If a KRP-by-SNC L_0 compatible with G_0 and u_i is secure against $\mathcal{E}^{adv} = \{\emptyset\}$, then at least one of subgraphs $G^{bn}_{s,i} \subset G_0$ must satisfy the following four requirements.

- R1 For $\beta \in \{0, 2\}$ each, the secret bits conveyed on the edges $e^{(\beta)}_{s,i}$ and $e^{(\beta+1)}_{s,i}$ are completely random and completely correlated, i.e., $I(S[e^{(\beta)}_{s,i}]; S[e^{(\beta+1)}_{s,i}]) = 1$.
- R2 The secret bit on $e^{(0)}_{s,i}$ is independent of that on $e^{(2)}_{s,i}$, i.e., $I(S[e^{(0)}_{s,i}]; S[e^{(2)}_{s,i}]) = 0$.
- R3 For $\beta \in \{0, 2\}$ each, $G^{bn}_{s,i}$ is the sender of the larger edge of $e^{(\beta)}_{s,i}$ and $e^{(\beta+1)}_{s,i}$.
- R4 $G^{bn}_{s,i}$ is the receiver of the second largest edge in the set $\{e^{(\alpha)}_{s,i}\}_{\alpha\in\{0,1,2,3\}}$.

We will prove this lemma in Section V-G.

However, we can also show that no KRP-by-SNC can satisfy such condition.

Lemma 7: In any KRP-by-SNC L_0 compatible with G_0 and u_i, no subgraph $G^{bn}_{s,i}$ can satisfy the four requirements R1, …, R4 of Lemma 6 simultaneously.

This is a contradiction, and thus, a secure L_0 cannot exist. This completes the proof of Lemma 4.

Proof of Lemma 7: We suppose that one of subgraphs $G^{bn}_{s,i}$ satisfies R1, …, R4, and derive a contradiction.

Below, as we concentrate on one such $G^{bn}_{s,i}$ satisfying R1, …, R4, we omit subscripts s, i for ease of notation, on the subgraph $G^{bn}_{s,i}$, edges $e^{(\alpha)}_{s,i}$, and nodes $v^{(\alpha)}_{s,i}$. Also, as KRP-by-SNC here uses only one type of channels, SC_e, we will often identify an edge e with the secret channel SC_e.

First note that the pair of the two largest edges in $\{e^{(\alpha)}\}_{\alpha\in\{0,1,2,3\}}$ must either be $e^{(0)}$ and $e^{(1)}$, or be $e^{(2)}$ and $e^{(3)}$. This is because if it is not the case, then R3 says that $G^{bn}(= G^{bn}_{s,i})$ is the sender of the second largest edge, but this contradicts R4. Thus, out of 6! types as the order of $e^{(0)}$, $e^{(1)}$, $e^{(2)}$, and $e^{(3)}$, it is sufficient to consider only eight types that satisfy the aforementioned condition.

Conditions R1, ⋯ , R4 as well as the structure of the subgraph G^{bn} are invariant under transpositions ($e^{(0)} \leftrightarrow e^{(1)}$ and $e^{(2)} \leftrightarrow e^{(3)}$) and ($e^{(0)} \leftrightarrow e^{(2)}$ and $e^{(1)} \leftrightarrow e^{(3)}$). Hence, there is a contradiction in the case of $e^{(0)} \prec e^{(1)} \prec e^{(2)} \prec e^{(3)}$, if and only if there exists a contradiction in all of other three cases $e^{(1)} \prec e^{(0)} \prec e^{(3)} \prec e^{(2)}$, $e^{(2)} \prec e^{(3)} \prec e^{(0)} \prec e^{(1)}$, and

$e^{(3)} \prec e^{(2)} \prec e^{(1)} \prec e^{(0)}$. Similarly, there is a contradiction in the case of $e^{(1)} \prec e^{(0)} \prec e^{(2)} \prec e^{(3)}$, if and only if there exists a contradiction in all of other three cases $e^{(0)} \prec e^{(1)} \prec e^{(3)} \prec e^{(2)}$, $e^{(2)} \prec e^{(3)} \prec e^{(1)} \prec e^{(0)}$, and $e^{(3)} \prec e^{(2)} \prec e^{(0)} \prec e^{(1)}$.

Therefore, we only have to consider the two cases

Case 1) $e^{(b)} \prec e^{(1-b)} \prec e^{(2)} \prec e^{(3)}$;

where $b = 0$ or 1 and derive a contradiction. Due to R1 and R2, we have

2) $I(S[e^{(0)}]; S[e^{(1)}]) = 1$;
3) $I(S[e^{(2)}]; S[e^{(3)}]) = 1$;
4) $I(S[e^{(0)}]; S[e^{(2)}]) = 0$.

G^{bn} must be the sender of edges $e^{(1-b)}$ and $e^{(3)}$ due to R3, and the receiver of $e^{(2)}$ due to R4. Thus, we have

5) $v^{(1-b)}$ is the sender of $e^{(1-b)}$;
6) $v^{(2)}$ is the receiver of $e^{(2)}$;
7) $v^{(3)}$ is the sender of $e^{(3)}$.

From the aforementioned relations 1),...,7), we can also prove the following two relations:

8) there exists a series of edges connecting $v^{(0)}$ and $v^{(1)}$ inside G^{bn} (e.g., $e^{(4)}$, $e^{(7)}$, and $e^{(10)}$) that are all smaller than $e^{(1-b)}$;
9) there exists a series of edges connecting $v^{(2)}$ and $v^{(3)}$ inside G^{bn} (e.g., $e^{(5)}$, $e^{(7)}$, and $e^{(9)}$) that are all larger than $e^{(2)}$ and all smaller than $e^{(3)}$.

However, these two relations contradict each other, and thus, Lemma 7 is proved.

Item 8) is obtained as follows. In order to realize relations 1), 2), and 5), the information of the secret bit on $e^{(b)}$ must be transferred from $v^{(b)}$ to $v^{(1-b)}$ inside G^{bn} before using the edge $e^{(1-b)}$. For this transfer, a series of edges connecting $v^{(0)}$ and $v^{(1)}$ must be used. Here, we have used the fact that there is no correlation between nodes before executing protocol L_0.

Item 9) is obtained as follows. Relations 2) and 4) imply that $I(S[e^{(0)}], S[e^{(1)}]; S[e^{(2)}]) = 0$. Combining this fact and relations 1) and 6), we find, that before the secret channel on $e^{(2)}$ is used, any random variable obtained on the nodes $\{v^{(\alpha)}\}_\alpha$ is independent of $S[e^{(2)}]$. As a result, relations 1), 3), and 7) imply that the secret bit on $e^{(2)}$ must be transferred from $v^{(2)}$ to $v^{(3)}$ inside G^{bn} before $e^{(3)}$ is used (and of course after $e^{(2)}$ is used).

□

G. PROOF OF LEMMA 6

We first introduce the notion of the *standard path* along with three lemmas related with it, and then, use them to prove Lemma. 6

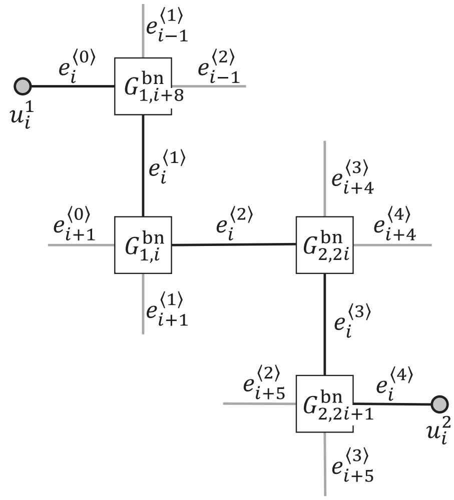

FIG. 13. Standard path i ($\in \{1, \ldots, 9\}$) consists of the five edges $\{e_i^{\langle\gamma\rangle}\}_{\gamma\in\{0,1,2,3,4\}}$, shown in black; also, see, Section V-G1. Note that each standard path i connects between user pair $u_i = (u_i^1, u_i^2)$. Note also that the graph G_0 of Fig. 10 is a disjoint union of these paths and subgraphs $G^{\text{bn}}_{s,i}$ (see Fig. 9), and that every subgraph $G^{\text{bn}}_{s,i}$ are connected to exactly two of these paths. As we will see in Lemma 8, in a secure KRP-by-SNC L_0, all the secret bits $S[e_i^{\langle\gamma\rangle}]$ transferred on the standard path i must equal the relayed key k_i^j, up to constants.

1) Standard Path and the Related Lemmas

The standard path is defined as follows.

Definition 9 (Standard Path $e_i^{\langle\gamma\rangle}$): For each user pair $u_i = (u_i^1, u_i^2)$, we define *standard path i* connecting them via subgraphs G^{bn} (more precisely, subgraphs $G^{\text{bn}}_{1,i+8}$, $G^{\text{bn}}_{1,i}$, $G^{\text{bn}}_{2,2i}$, and $G^{\text{bn}}_{2,2i+1}$) as in Fig. 13 . The standard path i consists of the following five edges:

$$\begin{aligned} e_i^{\langle 0\rangle} &:= e_{1,i+8}^{(2)} \\ e_i^{\langle 1\rangle} &:= e_{1,i+8}^{(3)} = e_{1,i}^{(0)} \\ e_i^{\langle 2\rangle} &:= e_{1,i}^{(1)} = e_{2,2i}^{(2)} \\ e_i^{\langle 3\rangle} &:= e_{2,2i}^{(3)} = e_{2,2i+1}^{(0)} \\ e_i^{\langle 4\rangle} &:= e_{2,2i+1}^{(1)}. \end{aligned} \tag{14}$$

We can show that all the edges $e_i^{\langle\gamma\rangle}$ on a standard path i convey essentially the same information, the relayed key k_i.

Lemma 8: In each standard path i, the secret bits $S[e_i^{\langle\gamma\rangle}]$ conveyed there must be equal to the relayed key $k_i^1 = k_i^2$ shared by the user pair u_i^1 and u_i^2 at the end points, up to constants. That is, for any i, j, and γ

$$S[e_i^{\langle\gamma\rangle}] = K_i^j \oplus d[e_i^{\langle\gamma\rangle}] \tag{15}$$

with $d[e_i^{\langle\gamma\rangle}]$ being constants.

We will prove this lemma in Section V-I.

Further, we can also show that k_i is first generated locally by one entity (a subgraph $G^{\text{bn}}_{i',s'}$ or a user u_i^j) on the standard path i, and then, repeatedly conveyed to an adjacent entity,

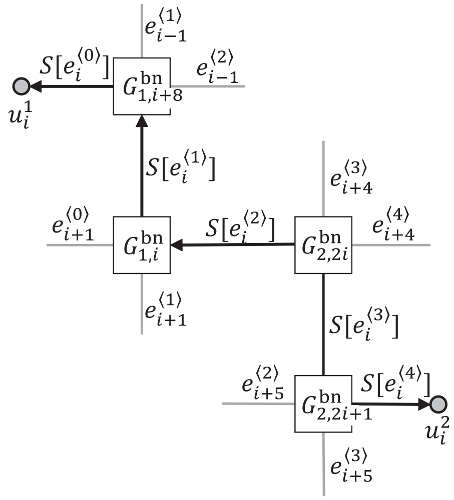

FIG. 14. Example of the flow of secret information $S[e_i^{\langle\beta\rangle}]$ on a standard path i, as stated in Lemma 9. Recall that all the secret bits $S[e_i^{\langle\beta\rangle}]$ transferred on the standard path i must equal the relayed key k_i^j, up to constants (Lemma 8 and Fig. 13). In the aforementioned example, k_i^j is first generated by $G_{2,2i}^{\rm bn}$ or by $G_{2,2i+1}^{\rm bn}$, and then, transferred via $e_i^{\langle 3\rangle}$. It is then repeatedly conveyed to an adjacent entity, until it is shared by the users u_i^1 and u_i^2 at the end points.

until it is shared by the users u_i^1 and u_i^2 at the end points; see Fig. 14. This phenomenon can be stated formally in terms of the ordering $\prec$ as follows.

Lemma 9: In each standard path i, the edges are used in the following manner. Let $e_i^{\langle\gamma_i\rangle}$ denote the first edge used.

1) Edges to the upper left of $e_i^{\langle\gamma_i\rangle}$ are used in order from lower right to upper left as

$$e_i^{\langle\gamma_i\rangle} \prec e_i^{\langle\gamma_i-1\rangle} \prec \cdots \prec e_i^{\langle 0\rangle} \tag{16}$$

and secret bits $S[e_i^{\langle\gamma\rangle}]$ on these edges besides $e_i^{\langle\gamma_i\rangle}$ flow left or upward.

2) Similarly, edges to the lower right of $e_i^{\langle\gamma_i\rangle}$ are used in order from upper left to lower right

$$e_i^{\langle\gamma_i\rangle} \prec e_i^{\langle\gamma_i+1\rangle} \prec \cdots \prec e_i^{\langle 4\rangle} \tag{17}$$

and secret bits $S[e_i^{\langle\gamma\rangle}]$ on these edges besides $e_i^{\langle\gamma_i\rangle}$ flow right or downward.

We will prove this lemma in Section V-J.

We can also show the following lemma.

Lemma 10: At least one of the following two conditions is false.

C1 For any subgraph $G_{s,i}^{\rm bn}$, $e_{s,i}^{(0)}$ or $e_{s,i}^{(1)}$ is the smallest edge in the standard path containing the two edges $e_{s,i}^{(0)}$ and $e_{s,i}^{(1)}$, when they are the two largest edges in $\{e_{s,i}^{(\alpha)}\}_{\alpha\in\{0,1,2,3\}}$.

C2 For any subgraph $G_{s,i}^{\rm bn}$, $e_{s,i}^{(2)}$ or $e_{s,i}^{(3)}$ is the smallest edge in the standard path containing the two edges $e_{s,i}^{(2)}$ and $e_{s,i}^{(3)}$, when they are the two largest edges in $\{e_{s,i}^{(\alpha)}\}_{\alpha\in\{0,1,2,3\}}$.

We will prove this lemma in Section V-K.

2) *Proof of Lemma 6*

From Lemma 8 (respectively, from Lemma 9), all the subgraph $G_{s,i}^{\rm bn}$ satisfy R1 and R2 (respectively, R3) in Lemma 6. Here, in order to derive R2, we used the mutual independence of $\{K_i^j\}_i$ additionally.

Hence, it remains to show that R4 holds for some $G_{s,i}^{\rm bn}$. To this end, we suppose that R4 does not hold for any $G_{s,i}^{\rm bn}$, and derive a contradiction with Lemma 10.

This is equivalent to showing, that in any subgraph $G_{s,i}^{\rm bn}$

1) C1 and C2 hold if R4 does not hold.

In the following, we will choose one of $G_{s,i}^{\rm bn}$ and show how to prove item (1). As $G_{s,i}^{\rm bn}$ is fixed, we omit subscripts s, i on the notation $e_{s,i}^{(\alpha)}$ for simplicity.

For the sake of the simplicity, we consider only the case of $e^{(0)} \prec e^{(1)}$ and $e^{(2)} \prec e^{(3)}$; all other cases can be shown similarly.

Then, we divide the remaining situation into the following three cases.

First, if the second largest edge in the set $\{e^{(\alpha)}\}_{\alpha\in\{0,1,2,3\}}$ is $e^{(1)}$ or $e^{(3)}$, the order $e^{(0)}, e^{(2)} \prec e^{(1)}, e^{(3)}$ must be derived from the assumptions $e^{(0)} \prec e^{(1)}$ and $e^{(2)} \prec e^{(3)}$, i.e., item (1) holds.

Second, if the second largest edge in the set $\{e^{(\alpha)}\}_\alpha$ is $e^{(0)}$, we find that $e^{(2)}, e^{(3)} \prec e^{(0)}, \prec e^{(1)}$ hold (as a result, C2 holds) and the sender of $e^{(0)}$ must be $G_{s,i}^{\rm bn}$. Here, we have used the assumption that R4 does not hold. From this fact and $e^{(0)} \prec e^{(1)}$, Lemma 9 guarantees that $e^{(0)}$ is the smallest edge in the standard path where it belongs, i.e., C1 holds. Thus, the item (1) also holds in this case.

Finally, if the second largest edge in the set $\{e^{(\alpha)}\}_\alpha$ is $e^{(2)}$, we can also show that item (1) holds in the same way as in the previous case.

This completes the proof of Lemma 6.

H. NOTE ON NOTATION: $v_{s,i}$ AND $E_0^{\rm st}$

In the proofs of Lemmas 8–10 given later, we only need to consider communication between subgraphs $G_{s,i}^{\rm bn}$, and do not need to refer to communication occurring inside each $G_{s,i}^{\rm bn}$. Therefore, in order to simplify the presentation, we will often denote a subgraph $G_{s,i}^{\rm bn}$ as a single node $v_{s,i}$. For example, the edge set $\{u_i^1, v_{s,i}\}$ denotes the set $\{u_i^1, v_{s,i}^{(0)}, v_{s,i}^{(1)}, v_{s,i}^{(2)}, v_{s,i}^{(3)}, v_{s,i}^{(4)}, v_{s,i}^{(5)}\}$.

Accordingly, we will also regard the graph G_0 as consisting of edges that connect nodes $v_{s,i}$ $(=G_{s,i}^{\rm bn})$ and u^i, which we denote by $E_0^{\rm st}$. This edge set $E_0^{\rm st}$ in fact consists of edges on the standard paths i, defined in the previous section

$$E_0^{\rm st} := \{e_i^{\langle\gamma\rangle}\}_{i\in\mathbb{Z}/9\mathbb{Z},\gamma\in\{0,1,2,3,4\}}. \tag{18}$$

I. PROOF OF LEMMA 8

1) Case of $e_i^{\langle 0\rangle}$

We divide nodes V_0 into u_i^1 and the others

$$V_i^{(1)} := \{u_i^1\} \tag{19}$$

$$\bar{V}_i^{(1)} := V_0 \backslash V_i^{(1)}. \tag{20}$$

Since these two sets are connected by $e_i^{\langle 0\rangle}$ only, there must be functions $f_i^{(j)}$ that satisfy the relation

$$f_i^{(1)}\left(S[e_i^{\langle 0\rangle}], \{C_v\}_{v\in V_i^{(1)}}\right) = K_i^1$$
$$= K_i^2 = f_i^{(2)}\left(S[e_i^{\langle 0\rangle}], \{C_v\}_{v\in \bar{V}_i^{(1)}}\right) \tag{21}$$

where C_v denotes all the random variables possessed by node $v \in V_0$ before executing protocol L_0. The first (last) equality in (21) comes from the facts that the node u_i^1 (u_i^2) are in the set $V_i^{(1)}(\bar{V}_i^{(1)})$. The second equality follows from the soundness of L_0.

Recall that the two sets $V_i^{(1)}$ and $\bar{V}_i^{(1)}$ are connected by $e_i^{\langle 0\rangle}$ only. Also, note that from the setting of the KRP-by-SNC, the secret bit $S[e_i^{\langle 0\rangle}]$ must be generated locally by the sender. Then, we have

$$I(S[e_i^{\langle 0\rangle}], \{C_v\}_{v\in V_i^{(1)}}; S[e_i^{\langle 0\rangle}], \{C_v\}_{v\in \bar{V}_i^{(1)}})$$
$$= H(S[e_i^{\langle 0\rangle}]). \tag{22}$$

Also, since $S[e_i^{\langle 0\rangle}]$ is one bit

$$H(S[e_i^{\langle 0\rangle}]) \le 1. \tag{23}$$

It remains to apply the following lemma to relations (21)–(23), and $H(K_i^j) = 1$.

Lemma 11: If B, C_0, and C_1 are random variables, and f_0 and f_1 are functions, satisfying

$$f_0(B, C_0) = f_1(B, C_1) =: A \tag{24}$$

$$H(A) \ge I(B, C_0; B, C_1) = H(B) \tag{25}$$

with $A \in \mathcal{A}$, $B \in \mathcal{B}$ where $|\mathcal{A}| = |\mathcal{B}|$, then there is a bijective function g such that $g(A) = B$.

Proof of this lemma is shown in Appendix. By using this lemma, we can find a bijective function g such that

$$S[e_i^{\langle 0\rangle}] = g\left(K_i^j\right). \tag{26}$$

In other words, we can find a certain constant values $d[e_i^{\langle 0\rangle}] \in \mathbb{Z}_2$ such that the relation

$$K_i^j = S[e_i^{\langle 0\rangle}] \oplus d[e_i^{\langle 0\rangle}] \tag{27}$$

holds for $i \in \mathbb{Z}/9\mathbb{Z}$ and $j \in \{1, 2\}$. When we apply the aforementioned Lemma 11, we have substituted K_i^j, $S[e_i^{\langle 0\rangle}]$, $\{C_v\}_{v\in V_i^{(1)}}$, and $\{C_v\}_{v\in \bar{V}_i^{(1)}}$ into A, B, C_0, and C_1 in Lemma, respectively.

Note, that from the constraint of soundness $K_i^1 = K_i^2$, we do not have to discriminate K_i^1 and K_i^2 hereafter. Therefore, we abbreviate the K_i^j into K_i in the following.

2) Case of $e_i^{\langle 4\rangle}$

This case can be shown completely in the same manner as the case of $e_i^{\langle 0\rangle}$. We have the relation

$$K_i = S[e_i^{\langle 4\rangle}] \oplus d[e_i^{\langle 4\rangle}] \tag{28}$$

for a certain constant $d[e_i^{\langle 4\rangle}]$.

3) Cases of $e_i^{\langle 1\rangle}$, $e_i^{\langle 2\rangle}$, and $e_i^{\langle 3\rangle}$

First, we use the same idea as in the case of $e_i^{\langle 0\rangle}$. We define the sets

$$V_i^{(3)} := \{u_{i+1}^1, u_{i+2}^1, u_{i+8}^2, u_{i+4}^2, u_i^2, u_{i+5}^2, v_{1,i}, v_{1,i+1}, v_{2,2i+8}, v_{2,2i}, v_{2,2i+1}, v_{2,2i+2}\} \tag{29}$$

$$V_i^{(4)} := \{u_{i+1}^1, u_{i+2}^1, u_{i+3}^1, u_{i+4}^2, u_i^2, u_{i+5}^2, v_{1,i}, v_{1,i+1}, v_{1,i+2}, v_{2,2i}, v_{2,2i+1}, v_{2,2i+2}\} \tag{30}$$

$$V_j^{(5)} := \{u_{i+1}^1, u_{i+2}^1, u_{i+3}^1, u_{i+4}^2, u_i^2, u_{i+5}^2, u_{i+6}^2, v_{1,i}, v_{1,i+1}, v_{1,i+2}, v_{2,2i}, v_{2,2i+1}, v_{2,2i+2}, v_{2,2i+4}\} \tag{31}$$

$$V_i^{(6)} := \{u_{i+1}^1, u_{i+2}^1, u_{i+6}^1, u_{i+4}^2, u_i^2, u_{i+5}^2, v_{1,i}, v_{1,i+1}, v_{1,i+5}, v_{2,2i}, v_{2,2i+1}, v_{2,2i+2}\} \tag{32}$$

and $\bar{V}_i^{(\mu)} := V_0 \backslash V_i^{(\mu)}$.

Since the two sets $V_i^{(3)}$ and $\bar{V}_i^{(3)}$ are connected only by $e_i^{\langle 1\rangle}$, $e_{i+2}^{\langle 1\rangle}$, $e_{i+1}^{\langle 3\rangle}$, $e_{i+8}^{\langle 3\rangle}$, $e_{i+4}^{\langle 2\rangle}$, and $e_{i+5}^{\langle 2\rangle}$, there exists a bijective function $g^{(3,i)}$

$$\left(S[e_i^{\langle 1\rangle}], S[e_{i+2}^{\langle 1\rangle}], S[e_{i+1}^{\langle 3\rangle}], S[e_{i+8}^{\langle 3\rangle}], S[e_{i+4}^{\langle 2\rangle}], S[e_{i+5}^{\langle 2\rangle}]\right)$$
$$= g^{(3,i)}\left(K_i, K_{i+1}, K_{i+2}, K_{i+4}, K_{i+5}, K_{i+8}\right). \tag{33}$$

Similarly, we have bijective functions $g^{(\mu,i)}$ for $\mu \in \{4, 5, 6\}$ and $i \in \mathbb{Z}/9\mathbb{Z}$ such that

$$\left(S[e_i^{\langle 1\rangle}], S[e_{i+3}^{\langle 1\rangle}], S[e_{i+4}^{\langle 3\rangle}], S[e_{i+1}^{\langle 3\rangle}], S[e_{i+2}^{\langle 2\rangle}], S[e_{i+5}^{\langle 2\rangle}]\right)$$
$$= g^{(4,i)}\left(K_i, K_{i+1}, K_{i+2}, K_{i+3}, K_{i+4}, K_{i+5}\right) \tag{34}$$

$$\left(S[e_i^{\langle 1\rangle}], S[e_{i+3}^{\langle 1\rangle}], S[e_{i+4}^{\langle 3\rangle}], S[e_{i+1}^{\langle 3\rangle}], S[e_{i+6}^{\langle 3\rangle}], S[e_{i+2}^{\langle 3\rangle}], S[e_{i+5}^{\langle 2\rangle}]\right)$$
$$= g^{(5,i)}\left(K_i, K_{i+1}, K_{i+2}, K_{i+3}, K_{i+4}, K_{i+5}, K_{i+6}\right) \tag{35}$$

$$\left(S[e_i^{\langle 1\rangle}], S[e_{i+2}^{\langle 1\rangle}], S[e_{i+5}^{\langle 1\rangle}], S[e_{i+6}^{\langle 1\rangle}], S[e_{i+4}^{\langle 3\rangle}], S[e_{i+1}^{\langle 3\rangle}]\right)$$
$$= g^{(6,i)}\left(K_i, K_{i+1}, K_{i+2}, K_{i+4}, K_{i+5}, K_{i+6}\right). \tag{36}$$

From these relations, we see that, for any $e \in E_0^{\mathrm{st}}$, random variable $S[e]$ is generated by at least one of bijective functions on a subset of $\{K_i\}_{i\in\mathbb{Z}/9\mathbb{Z}}$, i.e., (27), (28), and (33)–(36). This fact and the complete randomness of $\{K_i\}_i$ guarantee that the $S[e]$ must have the maximum entropy, i.e.,

$$H(S[e]) = 1. \tag{37}$$

for $e \in E_0^{\mathrm{st}}$.

Equations (33)–(36) allow to write the random variable $S[e_i^{\langle 1\rangle}]$ in multiple expressions as follows:

$$\begin{aligned}S[e_i^{\langle 1\rangle}] &= g_1^{(4,i)}(K_i, K_{i+1}, K_{i+2}, K_{i+3}, K_{i+4}, K_{i+5})\\ &= g_2^{(4,i+6)}(K_{i+6}, K_{i+7}, K_{i+8}, K_i, K_{i+1}, K_{i+2})\\ &= g_4^{(6,i+3)}(K_{i+3}, K_{i+4}, K_{i+5}, K_{i+7}, K_{i+8}, K_i).\end{aligned} \tag{38}$$

Here, $g_k^{(\mu,i)}(\cdot)$ denotes the kth element of the list of variables defined by the function $g^{\mu,i}(\cdot)$. From the complete randomness of $\{K_i\}_i$, $S[e_i^{\langle 1\rangle}]$ must depend only on the intersection of the sets as arguments of these functions

$$\begin{aligned}&\{K_i, K_{i+1}, K_{i+2}, K_{i+3}, K_{i+4}, K_{i+5}, \}\\ &\cap \{K_i, K_{i+1}, K_{i+2}, K_{i+6}, K_{i+7}, K_{i+8}\}\\ &\cap \{K_i, K_{i+3}, K_{i+4}, K_{i+5}, K_{i+7}, K_{i+8}\} = \{K_i\}.\end{aligned} \tag{39}$$

This fact and the relation (37) imply that

$$S[e_i^{\langle 1\rangle}] = K_i \oplus d[e_i^{\langle 1\rangle}] \tag{40}$$

for a certain constant $d[e_i^{\langle 1\rangle}]$.

In the same way, from the multiple representations of $S[e_i^{\langle 2\rangle}]$ and $S[e_i^{\langle 3\rangle}]$

$$\begin{aligned}S[e_i^{\langle 2\rangle}] &= g_5^{(3,i+5)}(K_{i+5}, K_{i+6}, K_{i+7}, K_i, K_{i+1}, K_{i+4})\\ &= g_6^{(3,i+4)}(K_{i+4}, K_{i+5}, K_{i+6}, K_{i+8}, K_i, K_{i+3})\\ &= g_5^{(4,i+7)}(K_{i+7}, K_{i+8}, K_i, K_{i+1}, K_{i+2}, K_{i+3})\end{aligned} \tag{41}$$

$$\begin{aligned}S[e_i^{\langle 3\rangle}] &= g_4^{(4,i+8)}(K_{i+8}, K_i, K_{i+1}, K_{i+2}, K_{i+3}, K_{i+4})\\ &= g_5^{(5,i+3)}(K_{i+3}, K_{i+4}, K_{i+5}, K_{i+6}, K_{i+7}, K_{i+8}, K_i)\\ &= g_5^{(6,i+5)}(K_{i+5}, K_{i+6}, K_{i+7}, K_i, K_{i+1}, K_{i+2})\end{aligned} \tag{42}$$

we can find that there are certain constants $d[e_i^{\langle\gamma\rangle}]$ such that the relation

$$S[e_i^{\langle\gamma\rangle}] = K_i \oplus d[e_i^{\langle\gamma\rangle}] \tag{43}$$

hold for $\gamma \in \{2, 3\}$.

Equations (27), (28), (40), and (43) prove the lemma.

J. PROOF OF LEMMA 9

Protocol L_0 can be viewed as a communication protocol performed by the subgraphs $G_{s,i}^{\mathrm{bn}}$ using the standard paths.

In this picture, the communication between $G_{s,i}^{\mathrm{bn}}$ satisfy the following properties.

1) Subgraphs $G_{s,i}^{\mathrm{bn}}$ are connected solely by the standard paths.
2) Each standard path i' is a straight line.
3) All edges in the standard path i' convey the same random bit $K_{i'}$, up to a constant (Lemma 8).
4) Random bits $K_{i'}$ are independent of each other (due to the definition of the KRP).

For these properties to hold, the following are necessary

1) Random bit $K_{i'}$ is generated inside one of subgraphs $G_{s,i}^{\mathrm{bn}}$ on the standard path i';
2) The value of $K_{i'}$, thus generated is conveyed repeatedly to adjacent subgraphs $G_{s,i}^{\mathrm{bn}}$ on the same standard path i'.

Thus the lemma holds.

Indeed, if 1) is not true, i.e., if $K_{i'}$ is generated independently by two or more of $G_{s,i}^{\mathrm{bn}}$, there is a nonzero probability that their values differ. For other subgraphs $G_{s,i}^{\mathrm{bn}}$ to be able to send out $K_{i'}$ thus generated, they must learn it from an adjacent subgraph which already knows $K_{i'}$.

K. PROOF OF LEMMA 10

We will take two steps.

First, we will show that, for any order $\prec$, there is a subset E' of E_0^{st}, which satisfies the following four items.

1) The subset E' contains the smallest edge in any standard path i.
2) $E_0^{\mathrm{st}} \neq E'$.
3) When $i \in \mathbb{Z}/9\mathbb{Z}$ is a value satisfying $e_i^{\langle\gamma\rangle}, e_{i+1}^{\langle\gamma'\rangle} \in E'$ for $\gamma \in \{1, 2\}$ and $\gamma' \in \{0, 1\}$, the relation $e_i^{\langle 3-\gamma\rangle}$, $e_{i+1}^{\langle 1-\gamma'\rangle} \in E'$ holds.
4) When $i \in \mathbb{Z}/9\mathbb{Z}$ is a value satisfying $e_i^{\langle\gamma\rangle}, e_{i+5}^{\langle\gamma'\rangle} \in E'$ for $\gamma \in \{3, 4\}$ and $\gamma' \in \{2, 3\}$, the relation $e_i^{\langle 7-\gamma\rangle}$, $e_{i+5}^{\langle 5-\gamma'\rangle} \in E'$ holds.

Second, we will show that the existence of E' defined previously and conditions C_1 and C_2 are incompatible for the order $\prec$ defined from a secure protocol L_0.

Thus, Lemma 10 holds.

The first step is shown as follows: We constructively show that for any sequence $\{\gamma_i \in \{0, 1, 2, 3, 4\}\}_{i\in\mathbb{Z}/9\mathbb{Z}}$, there is a subset that satisfies

1') $\forall i, \quad e_i^{\langle\gamma_i\rangle} \in E'$;

2)–4) such a subset is one of $E^{(1)}$, $E^{(2)}$, $E^{(3)}_{i,i'}$, and $E^{(4)}_q$ for $i \neq i' \in \mathbb{Z}/9\mathbb{Z}$ and $q \in \{0, 1, 2\}$ defined as follows:

$$E^{(1)} := \{e_i^{\langle\gamma\rangle} | i \in \mathbb{Z}/9\mathbb{Z}, \quad \gamma \in \{2, 3, 4\}\} \tag{44}$$

$$E^{(2)} := \{e_i^{\langle\gamma\rangle} | i \in \mathbb{Z}/9\mathbb{Z}, \quad \gamma \in \{0, 1, 2\}\} \tag{45}$$

$$E^{(3)}_{i',i''} := \left\{ e_i^{\langle\gamma\rangle} \left| \begin{array}{l} (i = i', \gamma \in \{0, 1\}) \\ \vee(i \in \{i'+1, i'+2, \dots, i''-1\}, \\ \qquad \gamma = 2) \\ \vee(i = i'', \gamma \in \{3, 4\}) \\ \vee(i \in \{i''+1, i''+2, \dots, i'+4\}, \\ \qquad \gamma \in \{0, 1, 2, 3, 4\}) \\ \vee(i \in \{i'+5, i'+6, \dots, i''+4\}, \\ \qquad \gamma \in \{0, 1, 2\}) \\ \vee(i \in \{i''+5, i''+6, \dots, i'+8\}, \\ \qquad \gamma \in \{0, 1, 2, 3, 4\}) \end{array} \right. \right\} \tag{46}$$

$$E^{(3)}_{i'',i'} := \left\{ e_i^{\langle\gamma\rangle} \;\middle|\; \begin{array}{l} (i = i', \gamma \in \{3,4\}) \\ \vee(i \in \{i'+1, i'+2, \ldots, i''-1\}, \\ \quad \gamma \in \{0,1,2,3,4\}) \\ \vee(i = i'', \gamma \in \{0,1\}) \\ \vee(i \in \{i''+1, i''+2, \ldots, j'+4\}, \\ \quad \gamma = 2) \\ \vee(i \in \{i'+5, i'+6, \ldots, i''+4\}, \\ \quad \gamma \in \{2,3,4\}) \\ \vee(i \in \{i''+5, i''+6, \ldots, i'+8\}, \\ \quad \gamma = 2) \end{array} \right\} \quad (47)$$

$$E^{(4)}_{q} := \left\{ e_i^{\langle\gamma\rangle} \;\middle|\; \begin{array}{l} (i \equiv q \bmod 3,\ \ \gamma \in \{0,1\}) \\ \wedge\ (i \equiv q+1 \bmod 3,\ \ \gamma \in \{2,3,4\}) \\ \wedge\ (i \equiv q+2 \bmod 3,\ \ \gamma \in \{3,4\}) \end{array} \right\} \quad (48)$$

where $i'' \in \{i'+1, i'+2, i'+3, i'+4\} \subset \mathbb{Z}/9\mathbb{Z}$. We can straightforwardly check that all the subsets satisfy the last three items 2)–4) directly. For any sequence $\{\gamma_j \in \{0,1,2,3,4\}\}_{j\in\mathbb{Z}/9\mathbb{Z}}$, we can find that one of the aforementioned subsets satisfies the item 1) as well. We confirmed this fact by a brute force search using a computer. This completes the first step of the proof.

For the second step, for any given order $\prec$ defined from a secure protocol L_0, we will derive a contradiction from the assumptions that conditions C1 and C2 hold and that there exists E', which satisfies the four items 1)–4). We pick up the smallest edge $e_{i_m}^{\langle\gamma_m\rangle}$ in $E_0^{\mathrm{st}}\backslash E'$. Existence of it guaranteed from the item 2). From the first item 1) and Lemma 9, there is a node $e_{i_m}^{\langle\gamma'\rangle} \in E'$ such that $|\gamma' - \gamma_m| = 1$.

When $\gamma', \gamma_m \in \{0,1\}$, we will give a contradiction, as an example. The third item 3) enforces

$$e_{i_m+8}^{\langle 1\rangle}, e_{i_m+8}^{\langle 2\rangle} \in E_0^{\mathrm{st}}\backslash E'. \quad (49)$$

From this relation and the minimality of $e_{i_m}^{\langle\gamma_m\rangle}$ in $E_0^{\mathrm{st}}\backslash E'$, the order $e_{i_m}^{\langle\gamma'\rangle} \prec e_{i_m}^{\langle\gamma_m\rangle} \prec e_{i_m+8}^{\langle 1\rangle}, e_{i_m+8}^{\langle 2\rangle}$ must hold. From this order, C1 enforces us that $e_{i_m+8}^{\langle 1\rangle}$ or $e_{i_m+8}^{\langle 2\rangle}$ must be a smallest edges in the standard path i_m+8. Here, we have use the facts that $e_{i_m}^{\langle\gamma'\rangle} = e_{1,i_m+8}^{(\gamma'+2)}$, $e_{i_m}^{\langle\gamma_m\rangle} = e_{1,i_m+8}^{(\gamma_m+2)}$, $e_{i_m+8}^{\langle 1\rangle} = e_{1,i_m+8}^{(0)}$, and $e_{i_m+8}^{\langle 2\rangle} = e_{1,i_m+8}^{(1)}$. As a result, the item 1) enforces us that $e_{i_m+8}^{\langle 1\rangle}$ or $e_{i_m+8}^{\langle 2\rangle}$ must be in E'. However, this relation contradicts the relation (49).

In the same way, we can derive contradictions in the other cases, i.e., $\gamma', \gamma_m \in \{1,2\}$ or $\gamma', \gamma_m \in \{2,3\}$ or $\gamma', \gamma_m \in \{3,4\}$.

VI. SUMMARY AND OUTLOOK

We investigated relations between the KRP and SNC under the one-shot scenario, as well as under the scenario where wiretap sets are restricted. We found that there is a definite gap in security between these two types of protocols; namely, certain KRPs achieve better security than any SNC schemes on the same graph. We also found that this gap can be closed by generalizing the notion of SNC by adding free public channels; that is, the KRP is equivalent to SNC augmented with free public channels.

There are still many open problems. For example, in Section IV, we gave only one counterexample, which is a 9-to-9 unicast situation where no node is compromised. On the other hand, it is an interesting open problem whether one can find other counterexamples in more general settings [19]. Another open problem is whether the gap we found here persist even under the asymptotic case.

It is also interesting to figure out on what types of graphs the gap occurs. Our conjecture is that there is no gap on plane graphs, and also for the case where there is only one sender–receiver pair, though the rigorous proofs remain as future works.

APPENDIX

FORMAL PROOF OF LEMMA 5

Proof: We prove the lemma by using a slightly modified protocol $L^{\mathrm{m}}_{\mathrm{KRP}}$, such that L_{KRP} being secure is equivalent to $L^{\mathrm{m}}_{\mathrm{KRP}}$ being secure.

$L^{\mathrm{m}}_{\mathrm{KRP}}$ is obtained by the following three process. First, when a public message made at any node in L_{KRP} can be expressed as a linear combination of the other public messages p_x and the local keys r_y held by the node, i.e., $\bigoplus_x p_x \oplus \bigoplus_y r_y$, the corresponding message made at the node in $L^{\mathrm{m}}_{\mathrm{KRP}}$ is a linear combination of the local keys r_y only, i.e., the parity of them $\bigoplus_y r_y$. Second, all the public communications in $L^{\mathrm{m}}_{\mathrm{KRP}}$ are used only for sending the parities to all users. Finally, as relayed keys, the users evaluate the same values as for L_{KRP}.

From this relation, we know that any bit obtained by the adversary in the case of $L^{\mathrm{m}}_{\mathrm{KRP}}$ can be evaluated by the adversary in the case of L_{KRP}, and vice versa. This is why L_{KRP} being secure is equivalent to $L^{\mathrm{m}}_{\mathrm{KRP}}$ being secure.

Self-contained definition of $L^{\mathrm{m}}_{\mathrm{KRP}}$ is as follows. $L^{\mathrm{m}}_{\mathrm{KRP}}$ is the protocol in which the following four phases are implemented in sequence.

1) *Local key generation phase:* All channels LKS_e are used to generate local keys.
2) *Parity evaluation phase:* Each node evaluates parities of (part of) local keys held by the node.
3) *Public communication phase:* Evaluated parities are transferred from each node to users via public communications.
4) *Relayed key generation phase:* Each user generates the relayed key from received local keys and the parities.

Parity evaluation phase and *relayed key generation phase* are explicitly identified by the following definitions.

1) *All the parities each nodes evaluate:* In each subgraph $G^{\mathrm{bn}}_{s,i}$, all the parities each nodes $v^{(\alpha)}$ evaluate are

$$v^{(0)}: \quad p[v^{(0)}, 1] := r[e^{(0)}] \oplus r[e^{(4)}] \quad (50)$$

$$p[v^{(0)}, 2] := r[e^{(4)}] \oplus r[e^{(6)}] \quad (51)$$

$$v^{(1)}: \quad p[v^{(1)}] := r[e^{(8)}] \oplus r[e^{(10)}] \oplus r[e^{(1)}] \tag{52}$$

$$v^{(2)}: \quad p[v^{(2)}, 1] := r[e^{(5)}] \oplus r[e^{(8)}] \tag{53}$$

$$p[v^{(2)}, 2] := r[e^{(2)}] \oplus r[e^{(5)}] \tag{54}$$

$$v^{(3)}: \quad p[v^{(3)}] := r[e^{(6)}] \oplus r[e^{(9)}] \oplus r[e^{(3)}] \tag{55}$$

$$v^{(4)}: \quad p[v^{(4)}] := r[e^{(4)}] \oplus r[e^{(5)}] \oplus r[e^{(7)}] \tag{56}$$

$$v^{(5)}: \quad p[v^{(5)}, 1] := r[e^{(7)}] \oplus r[e^{(10)}] \tag{57}$$

$$p[v^{(5)}, 2] := r[e^{(7)}] \oplus r[e^{(9)}]. \tag{58}$$

In order to simplify the next expression, we introduce the following notation:

$$p^{(0)}_{s,i} := p[v^{(0)}, 1] \oplus p[v^{(4)}] \oplus p[v^{(2)}, 1] \oplus p[v^{(5)}, 1] \oplus p[v^{(1)}] \tag{59}$$

$$p^{(1)}_{s,i} := p[v^{(2)}, 2] \oplus p[v^{(4)}] \oplus p[v^{(0)}, 2] \oplus p[v^{(5)}, 2] \oplus p[v^{(3)}]. \tag{60}$$

2) *The function which gives the relayed keys:* The relayed keys generated by u^1_i and u^2_i are

$$k^1_i := r[e^{(2)}_{1,i+8}] \tag{61}$$

$$k^2_i := p^{(1)}_{2,2i} \oplus p^{(1)}_{1,i+8} \oplus p^{(0)}_{1,i} \oplus p^{(0)}_{2,2i+1} \oplus r[e^{(1)}_{2,2i+1}] \tag{62}$$

for $i \in \mathbb{Z}/9\mathbb{Z}$.

From the definitions (50)–(60)

$$p^{(0)}_{s,i} = r[e^{(0)}_{s,i}] \oplus r[e^{(1)}_{s,i}] \tag{63}$$

$$p^{(1)}_{s,i} = r[e^{(2)}_{s,i}] \oplus r[e^{(3)}_{s,i}] \tag{64}$$

are obtained for each subgraph $G^{\mathrm{bn}}_{s,i}$. Here, we have used the fact that $r \oplus r = 0$ for $r \in \{0, 1\}$. By using the relations (63) and (64), the relayed keys (61) and (62) are evaluated as

$$k^1_i = k^2_i = r[e^{(2)}_{1,i+8}]. \tag{65}$$

This relation implies the soundness of L_{KRP}. Since the generated relayed keys are part of the local keys, and the public information is linear combinations of the local keys, the secrecy can be checked from the fact that the relayed keys are linearly independent of all the published information. □

PROOF OF LEMMA 11

From the assumption (24)

$$I(B, C_0; B, C_1) \geq I(A; B, C_1) \geq I(A; A) = H(A). \tag{66}$$

This relation and the assumption (25), guarantee that

$$I(B, C_0; B, C_1) = I(A; B, C_1) \tag{67}$$

$$H(A) = H(B). \tag{68}$$

The first relation and the assumption (24) imply

$$P(A = a)P(A = a, B = b, C_0 = c_0, C_1 = c_1) = P(A = a, B = b, C_0 = c_0)P(A = a, B = b, C_1 = c_1) \tag{69}$$

for any a, b, c_0, c_1. Here, we have used the fact that, if $I(Z; Y) = I(X; Y)$ for $Z := f(X)$, the relation $\forall x, y, z$, $P(X = x, Y = y, Z = z)P(Z = z) = P(X = x, Z = z)P(Y = y, Z = z)$ holds. By summing up with respect to c_1, the relation becomes

$$P(A = a, B = b, C_0 = c_0)P(A = a) = P(A = a, B = b, C_0 = c_0)P(A = a, B = b). \tag{70}$$

Since $A = f_0(B, C_0)$, we can define functions h_0 and h_1 such that $a = f_0(h_0(a), h_1(a))$ and $P(A = a, B = h_0(a), C_0 = h_1(a)) \neq 0$ hold, if $P(A = a) \neq 0$. Using these functions, by substituting $h_0(a)$ and $h_1(a)$ into b and c_0, respectively, in the aforementioned relation the following is attained:

$$P(A = a) = P(A = a, B = h_0(a)). \tag{71}$$

This relation guarantees the following relation:

$$\sum_{a,b} P(A = a, B = b)\delta(b, h_0(a)) = \sum_a P(A = a, B = h_0(a)) = \sum_a P(A = a) = 1 \tag{72}$$

i.e., $h_0(A) = B$. Therefore

$$I(A; B) = H(B) = H(A) \tag{73}$$

holds where (68) is used in the second equality. As a result, there is a function h_2 such that $h_2(B) = A$. The last assumption, i.e., the number of candidates for A is equal to that for B, and the existence of the functions h_0 and h_2 guarantee the existence of the bijective function g such that $g(A) = B$.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.*, vol. 92, May 2020, Art. no. 025002, doi: 10.1103/RevModPhys.92.025002.

[3] L. Salvail, M. Peev, E. Diamanti, R. Allèaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” *J. Comput. Secur.*, vol. 18, pp. 61–87, Jan. 2010, doi: 10.3233/JCS-2010-0373.

[4] R. Alléaume et al., “Using quantum key distribution for cryptographic purposes: A survey,” *Theor. Comput. Sci.*, vol. 560, pp. 62–81, 2014, doi: 10.1016/j.tcs.2014.09.018.

[5] T. R. Beals and B. C. Sanders, “Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network,” in *Information Theoretic Security*, R. Safavi-Naini, Ed. Berlin, Germany:Springer, 2008, pp. 29–39, doi: 10.1007/978-3-540-85093-9_4.

[6] *Overview on Networks Supporting Quantum Key Distribution*, *Int. Telecommun. Union*, Geneva, Switzerland, Recommendation Y.3800, Oct. 2019. [Online]. Available: http://handle.itu.int/11.1002/1000/11830-en

[7] OpenQKD, "Open European quantum key distribution testbed," doi: 10.3030/857156
[8] Chicago Quantum Exchange, "Chicago expands and activates quantum network, taking steps toward a secure quantum internet." [Online]. Available: https://news.uchicago.edu/story/chicago-quantum-network-argonne-pritzker-molecular-engineering-toshiba
[9] Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, pp. 214–219, 2021, doi: 10.1038/s41586-020-03093-8.
[10] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, May 2011, doi: 10.1364/OE.19.010387.
[11] N. Cai and R. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Inf. Theory*, 2002, Art. no. 323, doi: 10.1109/ISIT.2002.1023595.
[12] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with unequal link capacities and restricted wiretapping sets," in *Proc. IEEE Inf. Theory Workshop*, 2010, pp. 1–5, doi: 10.1109/CIG.2010.5592818.
[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008, doi: 10.1109/TIT.2008.921908.
[14] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed. London, U.K.: Chapman, 2020, doi: 10.1201/9781351133036.
[15] M. N. Wegman and J. Carter, "New Hash functions and their use in authentication and set equality," *J. Comput. Syst. Sci.*, vol. 22, no. 3, pp. 265–279, 1981, doi: 10.1016/0022-0000(81)90033-7.
[16] M. Hayashi, M. Owari, G. Kato, and N. Cai, "Reduction theorem for secrecy over linear network code for active attacks," *Entropy*, vol. 22, 2020, Art. no. 1053, doi: 10.3390/e22091053.
[17] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, "Resilient network coding in the presence of Byzantine adversaries," in *Proc. IEEE 26th Int. Conf. Comput. Commun.*, 2007, pp. 616–624, doi: 10.1109/INFCOM.2007.78.
[18] T. Ho and D. Lun, *Network Coding: An Introduction*. Cambridge, U.K.: Cambridge Univ. Press, 2008, doi: 10.1017/CBO9780511754623.
[19] H. Zhou, K. Lv, L. Huang, and X. Ma, "Quantum network: Security assessment and key management," *IEEE/ACM Trans. Netw.*, vol. 30, no. 3, pp. 1328–1339, Jun. 2022, doi: 10.1109/TNET.2021.3136943.

Go Kato was born in Japan, in 1976. He received the M.S. and Ph.D. degrees in science from The University of Tokyo, Tokyo, Japan, in 2001 and 2004, respectively.

In 2004, he joined the NTT Communication Science Laboratories and has been involved in the theoretical investigation of quantum information. His research interests include mathematical structures emerging in the field of quantum information. He moved to the National Institute of Information and Communication Technology, Tokyo, in 2022.

Dr. Kato is a Member of the Physical Society of Japan.

Mikio Fujiwara received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in physics from Nagoya University, Nagoya, Japan, in 1990, 1992, and 2002, respectively.

He has been involved in R&D activities with the National Institute of Information and Communications Technology (previous name CRL, Ministry of Posts and Telecommunications of Japan), Tokyo, Japan, since 1992.

Toyohiro Tsurumaru was born in Japan in 1973. He received the B.S. degree in physics from the University of Tokyo, Tokyo, Japan in 1996, and the M.S. and Ph.D. degrees in physics from the Graduate School of Science, University of Tokyo, in 1998 and 2001, respectively.

He has been with Mitsubishi Electric Corporation, Kamakura-shi, Japan since 2001. His research interests include the theoretical aspects of quantum cryptography and modern cryptography.