Simultaneously Generating Multiple Keys in Many to One Networks

Lifeng Lai and Lauren Huie

Abstract

The problem of simultaneously establishing multiple keys, one for each user in a set of users, is considered with possible assist from a group of dedicated helpers. This scenario arises when multiple users want to communicate securely with a base-station. For the case in which all users are required to generate keys, we develop a scheme that is sum rate optimal. For the case with dedicated helpers, we develop an achievable scheme and derive an outer bound. We identify conditions under which the developed scheme achieves the full capacity region and conditions under which it is sum rate optimal. We then specialize the study to a pairwise independent network model, for which we convert the key generation problem to a single-source multi-commodity flow over a network problem. Coupling results from graph theory, we fully characterize the capacity region for the general case of generating multiple keys with multiple helpers under the PIN model. Numerical examples are provided to illustrate the results derived in the paper.

Index Terms: Information theoretic security, Key generation, Multiple access

I. INTRODUCTION

Establishing secret keys to be shared by the sender and receiver in secure communications while keeping the keys secret from possible attackers is very challenging. Recently, a key agreement approach named key generation via public discussion has attracted considerable attention [1]–[5] under the source model and channel model. The basic setup of the so called source model is that two users namely Alice and Bob would like to establish a secret key

Lifeng Lai is with Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA, 01609. Email: llai@wpi.edu. Lauren Huie is with Air Force Research Lab, Information Directorate, Rome, NY, 13441. Email: Lauren.Huie@rl.af.mil. The work of L. Lai was supported by the National Science Foundation CAREER Award under Grant CCF-1054338, the National Science Foundation under Grant CNS-1116534, and Air Force Research Lab, Information Directorate.
between them by exchanging information in public. However, any such public discussion will be received by Eve perfectly. Surprisingly, it has been shown that, by public discussion, these two users can indeed establish a secret key such that Eve gains no information about the key, as long as these two users possess correlated but not necessarily the same random variables. These correlated random variables can be obtained from the random channel gains in wireless fading channels [6]–[12] or other sources. This line of work has been extended to models with an additional helper [3], a network with multiple helpers [2], and joint source-channel models [13], [14].

![Fig. 1. (a) Multiple cell phones need to establish separate keys with the base-station; (b) Multiple sensors need to establish pairwise keys for secure communications between them.](image)

Until now, with a few exceptions [15], [16], most of the existing work along this line focuses on generating a single key to be shared by a pair [1], [5] or a group of users [2]. In practice, however, there are various scenarios that require us to generate multiple keys to be shared by different pairs of users. For example, as shown in Figure 1 (a), in cellular systems, there are typically many wireless users, each of which needs to establish a key with the base-station to be used to protect the information exchanged between the wireless user and the base-station. Another example is shown in Figure 1 (b). In this example, multiple sensors in a sensor network need to establish pairwise keys for secure communications between them. In this paper, we focus on the many to one network as shown in Figure 1(a). In particular, we consider the problem of establishing multiple keys for multiple users, each to be shared by one user and the base station,
under the source model. Study of the model as shown in Figure 1(b) is left as future study (We have obtained some preliminary results regarding the model shown in Figure 1(b) in [17]).

A naive approach for this multiple-key establishment in the many to one network problem is to decompose this problem into multiple independent single-key generation problems. There are several issues with this approach. First, typically, the random sources at each user are correlated. Hence, the public discussion of user $i$ might leak information about the key established by user $j$. Hence, if one treats these problems separately, the keys may no longer be secure. Second, as shown in [2], [3], user cooperation can bring tremendous gains for the key generation. Hence, these multiple users can cooperate with each other to increase the key rate. As a result, this naive approach in which each user takes turns in generating keys might suffer performance losses.

In this paper, we rigorously formulate and provide solutions for the simultaneous multiple key generation problem. We first consider the scenario in which all the users are required to generate keys. We propose a scheme that is a careful concatenation of multiple modified single key generation problems. In the proposed scheme, users take turns to establish keys with user 0 (one can think of user 0 as the base station in Fig 1(a)) while treating all users that have finished the key generation process as colluding Eves who can share their observations. In each step, user $j$ sends enough information to user 0 such that user 0 is able to recover the observations at user $j$. As the result, user 0 accumulates more and more side information as the process continues, hence the users in the later steps sends less and less public discussion information to user 0. At the same time, Eve possesses more and more side-information. The key generation at each step is a modified single key generation problem with side-information at Eve such that the side-information is available to user 0 only. Each step is related to but different from two scenarios that have been studied in the literature: that of key generation with side information at Eve [1], in which Eve has additional correlated observations, and that of key generation with a helping Eve [1], [3], in which Eve reveals its observations to both users. The difference between this step and the standard key generation with side-information at Eve is that, in our case one of the legitimate users (specifically, user 0) knows the side-information at Eve. The difference between this step and the key generation with a helping Eve is that in our case only user 0 knows the observation at Eve, while in the key generation with a helping Eve, all users involved know the observation at Eve. We show that the public discussions in each step not only will not leak information about the key established in the same step when the public discussion occurs
but also will not leak information about the key established in other steps. Furthermore, we show that the combination of public information collected from these steps does not leak any information about these keys. We show that the proposed scheme is sum rate optimal. Here, we comment on the difference between this scenario and the existing work [15], [16] that considered the generation of two keys. In [15], [16], the key of each user needs to be secured from the other user. In our case, we do not impose this condition. Our setup is useful when the users in a network cooperate with each other in generating multiple keys, in the same spirit as the existing work on generating a single key with helpers [2], [3] such that the key is not required to be hidden from the helpers.

We then study the scenario in which there are several dedicated helpers whose sole goal is to assist the key generation process for other users. The achievable scheme developed in the previous scenario can be extended to this scenario with proper modifications. We also develop a general upper bound by extending techniques developed in [2]. We further identify cases under which the performance of the proposed scheme matches the outer bound, and conditions under which the proposed scheme is sum rate optimal.

We also specialize the study to the so called pairwise independent network (PIN) model [4], [18]. In the PIN model, the correlation between the random variables possess a certain structure, which arises naturally in generating keys using wireless fading gains. Exploiting this structure, we construct a graph based key generation approach. This approach has two steps. In the first step, we construct a graph by asking users in the network to establish pairwise local keys. In the second step, we use the local keys to propagate the keys from node 0 to other users. Our approach effectively converts the key generation problem to a single-source multi-commodity flow over a network problem. Leveraging results from graph theory [19], [20], we show that this graph based approach achieves the full capacity region for the general case of establishing multiple keys with the aid of multiple helpers.

The reminder of the paper is organized as follows. In Section II, we describe the model. In Section III, we study the case in which all users are required to generate keys. In Section IV, we note that [2] also considers the case in which the key is required to be hidden from the helpers. The extension to this setup along the line of [15], [16] is important and interesting. However, we note that the extension along this line is a generalization of the problem of key generation with side-information at Eve, which itself is an open problem [1], [5]. Hence, the extension along this line will be challenging.
we present our results for the network with dedicated helpers. In Section V, we specialize the study to the PIN model. In Section VI, we provide examples to illustrate the results derived in this paper. In Section VII, we offer conclusion remarks and point out possible future directions.

II. MODEL

![System model diagram]

The model considered in this paper is shown in Figure 2. In particular, we consider a scenario with $J + 1$ users, indexed by $j \in J \triangleq \{0, \cdots, J\}$. Each user $j \in M \triangleq \{1, \cdots, M\}$ needs to establish a key $K_j$ with user $0$. Users indexed by $j \in \{M + 1, \cdots, J\}$ act as dedicated helpers whose only purpose is to help the key generation process of the users in $M$. Hence, in our problem, we need to generate $M$ keys with $J - M$ dedicated helpers. One can think of user $0$ as the base station in the cellular system. Each user observes a random sequence $X^n_j$ taken from a set $\mathcal{X}_j$ with a finite alphabet size $|\mathcal{X}_j|$. The observations are correlated among the users but are independent and identically distributed (i.i.d.) over time. That is

\[
P_{X^n_0, \cdots, X^n_J}(x^n_0, \cdots, x^n_J) = \prod_{t=1}^{n} P_{X^n_0, \cdots, X^n_J}(x_0(t), \cdots, x_J(t)).
\]

These users are allowed to exchange information with each other in public. Without loss of generality, one can assume that these users take turns in sending public information for $r$ rounds.

\[^2\text{In this paper, we use capital letters to denote random variables, and lower case letters to denote the realization of the random variables.}\]
We use \( f_1, \cdots, f_{(J+1)} \) to denote the public information exchanged. Here, \( f_t \) is the information sent by user \( i = t \mod (J+1) \) at time \( t \). \( f_t \) depends on the random sequences \( X_i^n \) at user \( i \) and the public discussion \( f_1, \cdots, f_{t-1} \) that has occurred so far. We use \( F_j \) to denote the collection of public discussion sent by \( j \) during the public discussion phase, and \( F = [F_0, \cdots, F_J] \) to denote the whole set of public discussion. Eve knows the functions used at each user for generating the public information, and knows \( F \) perfectly.

After the public discussion is finished, by combining the public information \( F \) and its random sequence \( X^n_j \), user \( j \in \mathcal{M} \) generates a key \( K^*_{j} \) using a function \( g_j \), that is

\[
K^*_{j} = g_j(F, X^n_j).
\]  

(2)

Correspondingly, user 0 also generates a key \( K^0_{0} \), using \( X^n_0 \) and \( F \). We require that for each \( j \),

\[
\Pr\{K^*_{j} \neq K^0_{0}\} \leq \epsilon.
\]  

(3)

The condition (3) implies that the key generated at user \( j \) and 0 are the same with a high probability. In the following, we will use \( K_j \) to denote this common key shared by user \( j \) and 0. In total, we will generate \( M \) keys \( K_1, \cdots, K_M \), one for each user \( j \in \mathcal{M} \) to be shared with user 0.

In addition, we require

\[
\frac{1}{n} I(K_1, \cdots, K_M; F) \leq \epsilon.
\]  

(4)

This condition implies that Eve gains negligible amount of information about the keys \( K_1, \cdots, K_M \).

**Remark 1:** We note that (4) implies a weak notion of secrecy. To achieve a strong notion of secrecy, one would require \( I(K_1, \cdots, K_M; F) \leq \epsilon \). However, once we establish keys under the weak notion of secrecy, we can follow the approach in [21] to obtain keys with strong secrecy without sacrificing the key rate.

In addition to (3) and (4), we further require that these \( M \) keys to be uniformly distributed and independent of each other.

**Remark 2:** For secrecy purpose, it is not sufficient to guarantee the secrecy of individual keys and independence of keys. That is the following secrecy condition along with independence requirement are not sufficient for our multiple key generation problem:

\[
\frac{1}{n} I(K_j; F) \leq \epsilon, j = 1, \cdots, M.
\]  

(5)
To illustrate this, consider the case when $M = J = 2$ and $K_1$ and $K_2$ are two independent keys (equal size) for user 1 and user 2 respectively. Thus, we have $I(K_1; K_1 \oplus K_2) = 0$ and $I(K_2; K_1 \oplus K_2) = 0$. This implies that $K_1 \oplus K_2$ satisfies the condition (5). However, it is easy to check that $I(K_1, K_2; K_1 \oplus K_2) = H(K_1)$. This example implies that even if $F$ does not leak information about each individual key, the public discussion $F$ might still leak a significant amount of information about these $M$ keys. Hence, when we design our key generation schemes, we need to satisfy condition (4).

We say that a rate vector $(R_1, \cdots, R_M)$ is achievable, if there exists a public discussion scheme such that the above mentioned conditions are satisfied and

$$\frac{1}{n} H(K_j) \geq R_j - \epsilon.$$  \hfill (6)

The set of all achievable key rate vectors is called the key-rate region $C$. We will also be interested in the sum of these key rates, and refer to the largest possible sum rate as the sum key rate capacity:

$$C_{sum} = \sup_{(R_1, \cdots, R_M) \in C} \sum_{j=1}^{M} R_j.$$  \hfill (7)

In this paper, we are interested in characterizing $C$ and $C_{sum}$.

III. NO DEDICATED HELPERS

We first start with the case in which all users in the network are required to generate keys, i.e., there are no dedicated helpers hence $M = J$. In this section, we focus on characterizing the maximum sum key rate $C_{sum}$. Here, we provide a scheme that is sum-rate optimal. Before presenting the technical details, we provide an outline of the scheme. Our scheme is a careful concatenation of multiple rounds of modified single key generation problem. Without loss of generality, we start with user $J$. At first, user $J$ and user 0 generate the key $K_J$ with a rate $I(X_0; X_J)$ using the correlation $(X^n_J, X^n_0)$ and ignoring all other users. This is a single key generation problem [1], [5]. Let $F_J$ be the public discussion sent by user $J$ at this step. The existing single key generation scheme can guarantee that $I(K_J; F_J) \leq \epsilon$. In addition, by the end of this step, user 0 can recover $X^n_0$. At the second step, user $J - 1$ and user 0 generate the key $K_{J-1}$ with rate $I(X_0; X_{J-1}|X_J)$ by treating user $J$ as an Eve. This is a modified single key generation problem in the sense that Eve (user $J$) has additional side-information $(X^n_J)$.
and one of the legitimate users (user 0) has Eve’s side-information. It can be shown that there exists $F_{J-1}$ (the public information sent by user $J-1$) and $K_{J-1} = g_{X_{J-1}}(X_{J-1}^n)$ such that $I(K_{J-1}; F_{J-1}, X_{J-1}^n) \leq n\epsilon$. Furthermore, by the end of this step, user 0 is able to recover $X_{J-1}^n$.

At the third step, user $J-2$ and user 0 generate the key $K_{J-2}$ with rate $I(X_0; X_{J-2}|X_{J-1}, X_J)$ by treating users $J-1$ and $J$ as colluding Eves. Here, by colluding Eves, we mean that user $J-1$ and $J$ creates a super-Eve with side-information $(X_{J-1}^n, X_J^n)$. Again, this is a modified single key generation problem in the sense that Eve (super Eve created from users $J-1$ and $J$) has additional side-information $(X_{J-1}^n, X_J^n)$ and one of the legitimate users (user 0) has Eve’s side-information. It can be shown that there exists $F_{J-2}$ (the public information sent by user $J-2$) and $K_{J-2} = g_{X_{J-2}}(X_{J-2}^n)$ such that $I(K_{J-2}; F_{J-2}, X_{J-1}^n, X_J^n) \leq n\epsilon$. In addition, by the end of this step, user 0 will be able to recover $X_{J-2}^n$. This process continues until we reach user 1. In summary, each user takes turns in establishing keys with user 0 while treating all users that have finished the key establishment steps as colluding Eves with side-information. Each step is a modified single-key generation problem such that Eve has additional side-information, which is also available only at user 0. Furthermore, the amount of side-information increases as the process progresses. While it is relatively simple to guarantee that the public discussion in each step does not leak information about the key generated at that particular step, it does not automatically guarantee that this public discussion will not leak information about keys generated at other steps. Furthermore, the requirement in our system model is more strict. We require that the collection of all public discussions do not leak any information about all the keys. Our proof shows our scheme satisfies the security requirement (4). Figure 3 illustrates the outline of the scheme.

Before presenting the result, we state a lemma from [2] (with a slightly different notation and presentation) that will be used in the proof.

**Lemma 3 (Lemma B.3 in [2]):** Given i.i.d. repetitions $(U^n, V^n)$ of a pair of random variables $(U, V)$, and a positive number $H < H(U|V)$, for any function $F(U^n)$ of $U^n$ with cardinality $|F| \leq \exp(nH)$, any given $\epsilon$ and a given number $R$ satisfying

$$R \leq H(U|V) - H,$$

the probability that there exists a function $G(U^n)$ with the following properties goes to one as $n$ increases:
Fig. 3. An outline of the key generation scheme.

- \( G(U^n) \) is (arbitrarily close to) uniformly distributed over \( \{1, \cdots, \exp(nR)\} \):
  \[
  nR - \log||G(U^n)|| \leq \epsilon, \tag{9}
  \]
- \( G(U^n) \) is (arbitrarily close to) independent of \( (F(U^n), V^n) \):
  \[
  I(G(U^n); F(U^n), V^n) \leq \epsilon. \tag{10}
  \]

**Remark 4:** This lemma implies that the rate of \( G(U^n) \) is \( R \), furthermore, \( G(U^n) \) is uniformly distributed, and is independent of \( (F(U^n), V^n) \).

**Theorem 5:** The sum key rate capacity for generating \( J \) keys without dedicated helpers is

\[
C_{\text{sum}} = I(X_0; X_1, \cdots, X_J). \tag{11}
\]

**Proof:** **Converse:** We construct a genie-aided model by creating a super node \( 1' \) that combines all the observations at users \( \{1, \cdots, J\} \). We require user 0 and this super node \( 1' \) to create a single key \( K_1' \) with a rate \( R_1' \). This is a point-to-point scenario, and hence we know that

\[
R_1' \leq I(X_0; X_1, \cdots, X_J). \tag{12}
\]

It is clear that any scheme for the original model can be used to generate \( K_1' \) with a rate \( \sum_{j=1}^{J} R_j \). Applying the above bound, we have

\[
\sum_{j=1}^{J} R_j \leq I(X_0; X_1, \cdots, X_J). \tag{13}
\]
Achievability: We now show that the above genie-aided bound is indeed achievable.

In the following we use \([i, j]\) to denote \(\{i, i + 1, \ldots, j\}\), and \(X^n_{[i,j]}\) to denote \(\{X^i, \ldots, X^n\}\). For each user \(j \in \{1, \ldots, J\}\), consider random partitions of \(X^n\) to \(b_j\) bins. For each \(x^n_j \in X^n_j\), let \(f_{X_j}(x^n_j)\) be the index of the bin containing \(x^n_j\). Set
\[
\frac{1}{n} \log b_j = H(X_j|X_0, X_{[j+1,J]}) + \epsilon. \tag{14}
\]
User \(j\) sends \(f_{X_j}(X^n_j)\).

In Appendix A, we show that, from \((X^n_0, f_{X_1}(X^n_1), \ldots, f_{X_j}(X^n_j))\), user 0 can obtain an estimate \((\hat{X}^n_1, \ldots, \hat{X}^n_J)\) such that
\[
\Pr\{ (\hat{X}^n_1, \ldots, \hat{X}^n_J) \neq (X^n_1, \ldots, X^n_J) \} \leq \epsilon. \tag{15}
\]

The key generation process starts with user \(J\) and continues with a descending index order. For user \(j\), it will treat users from \(j + 1\) to \(J\) as colluding Eves in the sense that these users can share their observations. Now, using Lemma 3 (setting \(U = X_j, V = X_{[j+1,J]}\), \(F(U^n) = f_{X_j}(X^n_j)\)), we know that from \(X^n_j\), there exists a function \(g_{X_j}(X^n_j)\) distributed over \(\{1, 2, \ldots, 2^{nR_j}\}\) such that \(g_{X_j}(X^n_j)\) is nearly uniformly distributed, and
\[
I(g_{X_j}(X^n_j); f_{X_j}(X^n_j), X^n_{[j+1,J]}) \leq \epsilon,
\]
as long as
\[
R_j + \frac{1}{n} \log b_j \leq H(X_j|X_{[j+1,J]}). \tag{16}
\]
We set \(K_j = g_{X_j}(X^n_j)\), hence
\[
R_j = H(X_j|X_{[j+1,J]}) - H(X_j|X_0, X_{[j+1,J]}) - \epsilon = I(X_0; X_j|X_{[j+1,J]}) - \epsilon. \tag{17}
\]

Although the scheme is simple, the challenge lies in the security analysis. Now, we calculate the security level. It is clear that \(F = (f_{X_1}(X^n_1), \ldots, f_{X_J}(X^n_J))\).

\[
I(K_1, \ldots, K_J; F) = \sum_{j=1}^{J} I(K_j; F|K_{[j+1,J]}) \tag{18}
\]
\[
\leq \sum_{j=1}^{J} I(K_j; F, K_{[j+1,J]}) \tag{19}
\]
\[
\leq \sum_{j=1}^{J} I(K_j; f_{X_1}(X^n_1), \ldots, f_{X_J}(X^n_J), X^n_{[j+1,J]}). \tag{20}
\]
We now examine each term in the summation carefully.

\[
I(K_j; fX_1(X^n_1), \ldots, fX_j(X^n_j), X^n_{[j+1,j]})
\]
\[
= I(K_j; fX_j(X^n_j), X^n_{[j+1,j]}) + I(K_j; fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1})|fX_j(X^n_j), X^n_{[j+1,j]})
\]
\[
\leq I(K_j; fX_j(X^n_j), X^n_{[j+1,j]}) + I(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); K_j, fX_j(X^n_j), X^n_{[j+1,j]})
\]
\[
\leq I(K_j; fX_j(X^n_j), X^n_{[j+1,j]}) + I(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_j, X^n_{[j+1,j]})
\]
\[
\leq \epsilon + I(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_{[j+1,j]}).
\]  

In the following, we show that \(I(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_{[j+1,j]})\) is small. To proceed, from Fano’s inequality, we have

\[
H(X^n_1, \ldots, X^n_{j-1}|fX_1(X^n_1), \ldots, fX_j(X^n_j), X^n_j) \leq h_0(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |\mathcal{X}_i|.
\]  

We have

\[
H(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}))
\]
\[
\leq \sum_{i=1}^{j-1} H(fX_i(X^n_i))
\]
\[
= \sum_{i=1}^{j-1} n[H(X_i|X_0, X_{i+1}, \ldots, X_j) + \epsilon]
\]
\[
= nH(X_1, \ldots, X_{j-1}|X_0, X_j, \ldots, X_j) + n(j-1)\epsilon
\]
\[
= H(X^n_1, \ldots, X^n_{j-1}|X^n_0, X^n_j, \ldots, X^n_j) + n(j-1)\epsilon
\]
\[
= H(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_0, X^n_j, \ldots, X^n_j) + n(j-1)\epsilon
\]
\[
+ H(X^n_1, \ldots, X^n_{j-1}|fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_0, X^n_j, \ldots, X^n_j) + n(j-1)\epsilon
\]
\[
\leq H(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_0, X^n_j, \ldots, X^n_j)
\]
\[
+ n(j-1)\epsilon + h_0(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |\mathcal{X}_i|,
\]

which implies that

\[
I(fX_1(X^n_1), \ldots, fX_{j-1}(X^n_{j-1}); X^n_0, X^n_{[j, j]}) \leq n(j-1)\epsilon + h_0(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |\mathcal{X}_i|.
\]
Hence,

\begin{align}
I(f_{X_1}(X_1^n), \cdots, f_{X_{j-1}}(X_{j-1}^n); X_{[j,j]}^n) \\
\leq I(f_{X_1}(X_1^n), \cdots, f_{X_{j-1}}(X_{j-1}^n); X_0^n, X_{[j,j]}^n) \\
\leq n(j - 1)\epsilon + h_b(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |X_i|.
\end{align}

(37) (38) (39)

Plugging (39) in (25), we have

\begin{align}
I(K_j; f_{X_1}(X_1^n), \cdots, f_{X_j}(X_j^n), X_{[j+1,J]}^n) \\
\leq \epsilon + I(f_{X_1}(X_1^n), \cdots, f_{X_{j-1}}(X_{j-1}^n); X_{[j,j]}^n) \\
\leq \epsilon + n(j - 1)\epsilon + h_b(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |X_i|.
\end{align}

(40) (41) (42)

Plugging (42) back to (20), we know that

\begin{align}
I(K_1, \cdots, K_J; F) \\
\leq \sum_{j=J}^{1} I(K_j; f_{X_1}(X_1^n), \cdots, f_{X_j}(X_j^n), X_{[j+1,J]}^n) \\
\leq \sum_{j=J}^{1} \left( \epsilon + n(j - 1)\epsilon + h_b(\epsilon) + n\epsilon \log \prod_{i=1}^{j-1} |X_i| \right).
\end{align}

(43) (44) (45)

From this, we know that the public discussion leaks a small amount of information about the generated keys. Furthermore, we have

\[
\sum_{j=1}^{J} R_j = \sum_{j=1}^{J} I(X_0; X_j|X_{[1,j-1]}) = I(X_0; X_1, \cdots, X_J). \tag{46}
\]

In addition, from the construction, we know that the keys are nearly uniformly distributed and the mutual information between the generated keys is arbitrarily small. The proof is complete.

We note that in the proof, the order of the process is from user $J$ to 1. It is easy to see that any order will allow us to achieve the sum-rate capacity. The convex hull of these $J!$ tuples, one for each possible order and each of them lies on the outer-bound, with $(0, \cdots, 0)$ consists of an inner bound of the whole capacity region.
IV. HELPER NODES

In this section, we discuss the case with dedicated helpers. Here, we note that in our model it is not required that the generated keys be kept secure from these helper nodes. In this section, we state the results for the case of $M = 2$ and $J = 3$ in detail. That is, in addition to users 0, 1 and 2, which are required to generate keys, there is another user that can help the establishment of key $K_1$ between user 0 and user 1, and key $K_2$ between user 0 and user 2. The results developed in this section can be generalized to any values of $M$ and $J$, but the form will be complicated\(^3\).

We will provide an achievable rate region by modifying the scheme used in the previous section. In addition, we also provide an outer bound. We then discuss cases under which the inner and outer bounds match, and cases under which the developed scheme is sum-rate optimal.

The scheme is a generalization of the scheme developed in the previous section. We have the following achievable rate region.

*Theorem 6:* The key capacity region of generating two keys with a dedicated helper is inner-bounded by the convex hull of the point $(0, 0)$ and the following four pairs of $(R_1, R_2)$:

\[
P_1 = \left(0, \min_{\{B \subseteq F : 0 \in B, 2 \notin B^c\}} I(X_B; X_{B^c})\right),
\]

\[
P_2 = (I(X_0; X_1|X_2, X_3), I(X_0; X_2|X_3) + \min\{I(X_0; X_3), I(X_2; X_3)\}),
\]

\[
P_3 = (I(X_0; X_1|X_3) + \min\{I(X_0; X_3), I(X_1; X_3)\}, I(X_0; X_2|X_1, X_3)),
\]

\[
P_4 = \left(\min_{\{B \subseteq F : 0 \in B, 1 \in B^c\}} I(X_B; X_{B^c}), 0\right).
\]

*Proof:*

$P_1$ ($P_4$) is achievable when one is required to generate only $K_2$ ($K_1$) \([2]\). In the following, we show that $P_2$ is achievable. This proof is an extension of the proof in Theorem 5 with proper modifications. The proof that $P_3$ is achievable is similar.

Consider random partitions of $X_1^n$, $X_2^n$ and $X_3^n$ into $b_1$, $b_2$ and $b_3$ bins. For each $x_i^n \in X_i^n$.

\(^3\)In the next section, we will address this general case under the PIN model. Under the PIN model, we show that the capacity region has a simple structure.
\(i = 1, 2, 3\), let \(f_{X_i}(x^n_i)\) be the index of the bin containing \(x^n_i\). Set
\[
\frac{1}{n} \log b_1 = H(X_1|X_0, X_2, X_3) + \epsilon, \quad (51)
\]
\[
\frac{1}{n} \log b_2 = H(X_2|X_0, X_3) + \epsilon, \quad (52)
\]
\[
\frac{1}{n} \log b_3 = \max\{H(X_3|X_0, H(X_3|X_2, X_3))\} + \epsilon. \quad (53)
\]

User \(i\) sends \(f_{X_i}(x^n_i)\). Using source coding with side information, we know that user 0 can obtain an estimate \((\hat{X}_1^n, \hat{X}_2^n, \hat{X}_3^n)\) from \((X_0^n, f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n))\) such that
\[
\Pr\{(\hat{X}_1^n, \hat{X}_2^n, \hat{X}_3^n) \neq (X_1^n, X_2^n, X_3^n)\} \leq \epsilon. \quad (54)
\]
Furthermore, from (53), we know that user 2 can obtain an estimate \(\tilde{X}_3^n\) from \((X_2^n, f_{X_3}(X_3^n))\) such that
\[
\Pr\{\tilde{X}_3^n \neq X_3^n\} \leq \epsilon. \quad (55)
\]

Now, using Lemma 3, we know that from \(X_1^n\), there exists a function \(g_{X_1}(X_1^n)\) with a (arbitrarily close to) uniform distribution over \(\{1, 2, \ldots, 2^{nR_1}\}\) such that
\[
I(g_{X_1}(X_1^n); f_{X_1}(X_1^n), X_2^n, X_3^n) \leq \epsilon,
\]
as long as
\[
R_1 + \frac{1}{n} \log b_1 \leq H(X_1|X_2, X_3). \quad (56)
\]
We set \(K_1 = g_{X_1}(X_1^n)\), hence
\[
R_1 = H(X_1|X_2, X_3) - H(X_1|X_0, X_2, X_3) - \epsilon = I(X_0; X_1|X_2, X_3) - \epsilon. \quad (57)
\]

Using Lemma 3, we know that from \(X_2^n\), there exists a function \(g_{X_2}(X_2^n)\) with a (arbitrarily close to) uniform distribution over \(\{1, 2, \ldots, 2^{nS_2}\}\) such that
\[
I(g_{X_2}(X_2^n); f_{X_2}(X_2^n), X_3^n) \leq \epsilon,
\]
as long as
\[
S_2 + \frac{1}{n} \log b_2 \leq H(X_2|X_3). \quad (58)
\]
We set \(K_2 = g_{X_2}(X_2^n)\), hence
\[
S_2 = H(X_2|X_3) - H(X_2|X_0, X_3) - \epsilon = I(X_0; X_2|X_3) - \epsilon. \quad (59)
\]
Using Lemma 3, we know that from $X_3^n$, there exists a function $g_{X_3}(X_3^n)$ with a (arbitrarily close to) uniform distribution over $\{1, 2, \cdots, 2^{nT_2}\}$ such that

$$I(g_{X_3}(X_3^n); f_{X_3}(X_3^n)) \leq \epsilon,$$

as long as

$$T_2 + \frac{1}{n} \log b_3 \leq H(X_3). \quad (60)$$

We set $K^b_2 = g_{X_3}(X_3^n)$, hence

$$T_2 = H(X_3) - \max\{H(X_3|X_0), H(X_3|X_2)\} - \epsilon = \min\{I(X_0; X_3), I(X_2; X_3)\} - \epsilon. \quad (61)$$

We set $K_2$ to be the concatenation of $K^a_2$ and $K^b_2$. Hence

$$R_2 = S_2 + T_2 = I(X_0; X_2|X_3) + \min\{I(X_0; X_3), I(X_2; X_3)\} - 2\epsilon.$$

Note that from (54) and (55), we know that both users 0 and 2 know $X_3^n$, hence both of them know $K^b_2$ and therefore $K_2$. Hence, in this scheme, user 3 effectively helps users 0 and 2 in generating keys.

Now, we calculate the security level. From the description of the scheme, we know that the public information that is available to Eve is

$$F = (f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n)). \quad (62)$$

We have

$$I(K_1, K_2; F) = I(K_2; F) + I(K_1; F|K_2) \leq I(K_2; F) + I(K_1; F, K_2) \leq I(K_2; F) + I(K_1; f_{X_1}(X_1^n), X_2^n, X_3^n). \quad (63)$$

We bound each term in (63). First, from the construction, we have

$$I(K_1; f_{X_1}(X_1^n), X_2^n, X_3^n) \leq \epsilon. \quad (64)$$

We now bound the term $I(K_2; F)$. First,

$$I(K^a_2; F) \quad (65)$$

$$= I(g_{X_2}(X_2^n); f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n)) \quad (66)$$

$$\leq I(g_{X_2}(X_2^n); f_{X_2}(X_2^n), f_{X_3}(X_3^n)) + I(f_{X_1}(X_1^n); g_{X_2}(X_2^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n)) \quad (67)$$

$$\leq \epsilon + I(f_{X_1}(X_1^n); X_2^n, X_3^n). \quad (68)$$
From Fano’s inequality, we have
\[
H(X_1^n | f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n), X_0^n) \leq h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1|.
\] (69)

Furthermore
\[
H(f_{X_1}(X_1^n)) \leq nH(X_1|X_0, X_2, X_3) + n\epsilon
\] (70)
\[
= H(X_1^n, f_{X_1}(X_1^n)|X_0^n, X_2^n, X_3^n) + n\epsilon
\] (71)
\[
= H(f_{X_1}(X_1^n)|X_0^n, X_2^n, X_3^n) + H(X_1^n|f_{X_1}(X_1^n), X_0^n, X_2^n, X_3^n) + n\epsilon
\] (72)
\[
\leq H(f_{X_1}(X_1^n)|X_0^n, X_2^n, X_3^n) + n\epsilon + h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1|.
\] (73)

Hence,
\[
I(f_{X_1}(X_1^n); X_0^n, X_2^n, X_3^n) \leq n\epsilon + h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1|.
\] (74)

We have
\[
I(K_2^a, f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n)) \leq \epsilon + I(f_{X_1}(X_1^n); X_0^n, X_3^n)
\] (75)
\[
\leq \epsilon + I(f_{X_1}(X_1^n); X_0^n, X_2^n, X_3^n)
\] (76)
\[
\leq \epsilon + n\epsilon + h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1|.
\] (77)

Similarly, we can show that
\[
I(K_2^b, f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n)) \leq 2\epsilon + n\epsilon + h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1||\mathcal{X}_2|.
\] (78)

Since $K_2^a = g_{X_2}(X_2^n)$ is independent of $X_0^n$, $K_2^b$ is independent of $K_2^b = g_{X_3}(X_3^n)$.

We have
\[
I(K_2; F) = I(K_2^a, K_2^b; F)
\] (79)
\[
= I(K_2^b; F) + I(K_2^a; F|K_2^b)
\] (80)
\[
\leq I(K_2^b; F) + I(K_2^a; F, K_2^b)
\] (81)
\[
= I(K_2^b; F) + I(K_2^a; f_{X_1}(X_1^n), f_{X_2}(X_2^n), f_{X_3}(X_3^n), g_{X_3}(X_3^n))
\] (82)
\[
\leq I(K_2^b; F) + I(K_2^a; f_{X_1}(X_1^n), f_{X_2}(X_2^n), X_3^n)
\] (83)
\[
\leq I(K_2^b; F) + I(K_2^a; f_{X_2}(X_2^n), X_3^n) + I(f_{X_1}(X_1^n); X_2^n, X_3^n)
\] (84)
\[
\leq 3\epsilon + 2n\epsilon + 2h_b(\epsilon) + n\epsilon \log |\mathcal{X}_1||\mathcal{X}_2| + n\epsilon \log |\mathcal{X}_1|.
\] (85)
By plugging (64) and (85) into (63), we know that Eve obtains a negligible amount of information about the generated keys.

Furthermore, since the mutual information between \( K_1 = g_{x_1}(X_1^n) \) and \( (X_2^n, X_3^n) \) is arbitrarily small, the mutual information between \( K_1 \) and \( K_2 = (g_{x_2}(X_2^n), g_{x_3}(X_3^n)) \) is arbitrarily small.

The following theorem provides an outer bound for the one helper scenario.

**Theorem 7:** The secret key rate region for generating two keys with a dedicated helper is outer bounded by the following region:

\[
\begin{align*}
R_1 & \leq \min_{\{B \subseteq \mathcal{J}, 0 \in B, 1 \in B^c\}} I(X_B; X_{B^c}), \\
R_2 & \leq \min_{\{B \subseteq \mathcal{J}, 0 \in B, 2 \in B^c\}} I(X_B; X_{B^c}), \\
R_1 + R_2 & \leq \min \{I(X_0; X_{\{0\}^c}), I(X_{\{0,3\}}; X_{\{1,2\}})\}, \\
R_1 + 2R_2 & \leq 2H(X_{\mathcal{J}}) - \\
& \max\{H(X_0 | X_{\{0\}^c}) + H(X_{\{1,2\}} | X_{\{0,3\}}) + H(X_{\{2,3\}} | X_{\{0,1\}}) + H(X_{\{1\}^c} | X_2), \\
& H(X_{\{0\}^c} | X_0) + H(X_{\{0,3\}} | X_{\{1,2\}}) + H(X_{\{0,1\}} | X_{\{2,3\}}) + H(X_2 | X_{\{2\}^c})\}\}
\end{align*}
\]

\[
2R_1 + R_2 \leq 2H(X_{\mathcal{J}}) - \\
\max\{H(X_0 | X_{\{0\}^c}) + H(X_{\{1,2\}} | X_{\{0,3\}}) + H(X_{\{1,3\}} | X_{\{0,2\}}) + H(X_{\{1\}^c} | X_1), \\
H(X_{\{0\}^c} | X_0) + H(X_{\{0,3\}} | X_{\{1,2\}}) + H(X_{\{0,2\}} | X_{\{1,3\}}) + H(X_1 | X_{\{1\}^c})\}.
\]

**Proof:** The proof is provided in Appendix B. 

As a consequence of this Theorem, we have the following tight result that shows our scheme achieves the full capacity under certain conditions.

**Lemma 8:** If

\[
I(X_0; X_1X_2X_3) = \min_{\{B \subseteq \mathcal{J}, 0 \in B, 1 \in B^c\}} I(X_B; X_{B^c}) = \min_{\{B \subseteq \mathcal{J}, 0 \in B, 2 \in B^c\}} I(X_B; X_{B^c}),
\]

the inner bound in Theorem 6 matches the outer bound in Theorem 7, and the capacity region is given by

\[
R_1 + R_2 \leq I(X_0; X_1X_2X_3).
\]

**Proof:** If (88) is satisfied, then \( P_1 \) is the same as \((I(X_0; X_1X_2X_3), 0)\), and \( P_4 \) is the same as \((0, I(X_0; X_1X_2X_3))\). Hence, by any point on the line connecting \( P_1 \) and \( P_4 \) is achievable,
and hence any \((R_1, R_2)\) pair satisfying
\[
R_1 + R_2 \leq I(X_0; X_1X_2X_3),
\]
is achievable.

Now, for outer bound, if (88) is true, we have
\[
I(X_0; X_1X_2X_3) \leq I(X_0X_3; X_1X_2).
\]
(91)
As a result, the first three equations in Theorem 7 give
\[
R_1 + R_2 \leq I(X_0; X_1X_2X_3),
\]
(92)
which matches the inner bound (90). Hence, the capacity region is given by (88).

The conditions in Lemma 8 are quite restrictive. We have the following less restrictive conditions under which our scheme is sum-rate optimal.

**Lemma 9:** If any of the following conditions are satisfied, the scheme in Theorem 6 is sum-rate optimal.

1) \(X_1 \rightarrow X_2 \rightarrow X_3\), or
2) \(I(X_0; X_3) \leq I(X_2; X_3)\), or
3) \(X_2 \rightarrow X_1 \rightarrow X_3\), or
4) \(I(X_0; X_3) \leq I(X_1; X_3)\).

**Proof:** We check each case one by one.

1) Case \(X_1 \rightarrow X_2 \rightarrow X_3\)

We focus on the sum rate upper bound in (86). First, one can verify that the following relationships are true:
\[
I(X_0; X_1X_2X_3) = I(X_0; X_2X_3) + I(X_0; X_1|X_2X_3),
\]
(93)
\[
I(X_0X_3; X_1X_2) = I(X_0X_3; X_2) + I(X_0X_3; X_1|X_2)
\]
(94)
\[
= I(X_2; X_0X_3) + I(X_3; X_1|X_2) + I(X_0; X_1|X_2X_3).
\]
(95)
Hence, if \(X_1 \rightarrow X_2 \rightarrow X_3\), \(I(X_1; X_3|X_2) = 0\), the sum rate bound in (86) becomes
\[
\min\{I(X_0; X_{\{0\}^c}), I(X_{\{0,3\}}; X_{\{1,2\}})\}
\]
\[
= I(X_0; X_1|X_2X_3) + \min\{I(X_0; X_2X_3), I(X_2; X_0X_3)\}
\]
\[
= I(X_0; X_1|X_2, X_3) + I(X_0; X_2|X_3) + \min\{I(X_0; X_3), I(X_2; X_3)\},
\]
(96)
which is achieved by Point \( P_2 \).

2) Case \( I(X_0; X_3) \leq I(X_2; X_3) \)

If \( I(X_0; X_3) \leq I(X_2; X_3) \), we have

\[
\min\{I(X_0; X_2X_3), I(X_2; X_0X_3)\} = I(X_0; X_2X_3).
\] (97)

From (95), we have

\[
\min\{I(X_0; X_{\{0\}^c}), I(X_{\{0,3\}^c}; X_{\{1,2\}^c})\} = I(X_0; X_1X_2X_3).
\] (98)

At the same time, the sum rate achievable by Point \( P_2 \) is

\[
I(X_0; X_1|X_2, X_3) + I(X_0; X_2|X_3) + \min\{I(X_0; X_3), I(X_2; X_3)\}
\]

\[
= I(X_0; X_1|X_2, X_3) + I(X_0; X_2|X_3) + I(X_0; X_3) = I(X_0; X_1X_2X_3),
\] (99)

which implies that \( P_2 \) achieves the sum rate.

3) Case \( X_2 \rightarrow X_1 \rightarrow X_3 \)

We focus on the sum rate bound in (86). First, one can verify that the following relationships are true:

\[
I(X_0; X_1X_2X_3) = I(X_0; X_1X_3) + I(X_0; X_2X_1X_3),
\] (100)

\[
I(X_0X_3; X_1X_2) = I(X_0X_3; X_1) + I(X_0X_3; X_2|X_1)
\]

\[
= I(X_1; X_0X_3) + I(X_3; X_2|X_1) + I(X_0; X_2|X_1X_3).
\] (102)

Hence, if \( X_2 \rightarrow X_1 \rightarrow X_3 \), \( I(X_2; X_3|X_1) = 0 \), the sum rate bound in (86) becomes

\[
\min\{I(X_0; X_{\{0\}^c}), I(X_{\{0,3\}^c}; X_{\{1,2\}^c})\}
\]

\[
= I(X_0; X_2|X_1X_3) + \min\{I(X_0; X_1X_3), I(X_1; X_0X_3)\}
\]

\[
= I(X_0; X_2|X_1X_3) + I(X_0; X_1|X_3) + \min\{I(X_0; X_3), I(X_1; X_3)\},
\] (103)

which is achieved by Point \( P_3 \).

4) Case \( I(X_0; X_3) \leq I(X_1; X_3) \)

Similar to the case of \( I(X_0; X_3) \leq I(X_2; X_3) \), one can verify that the sum-rate point can be achieved by point \( P_3 \).
In the following, we discuss the case of generating two keys without helpers. This can be viewed as a special case of the above scenario by setting $X_3 = \Phi$. The discussion will be useful for the discussion in the next section. In the following, we will use $A = I(X_0; X_1X_2)$, $B = I(X_1; X_0X_2)$ and $C = I(X_2; X_0X_1)$. In particular, we have

**Lemma 10:** The region for the case of generating two keys without helpers is inner bounded by the convex hull of the point $(0, 0)$ and the following four pairs of $(R_1, R_2)$:

\[
\begin{align*}
P_1 &= (0, \min\{A, C\}), \\
P_2 &= (I(X_0; X_1X_2), I(X_0; X_2)), \\
P_3 &= (I(X_0; X_1), I(X_0; X_2X_1)), \\
P_4 &= (\min\{A, B\}, 0).
\end{align*}
\]

Furthermore, the region is outer bounded by

\[
\begin{align*}
R_1 &\leq \min\{A, B\}, \\
R_2 &\leq \min\{A, C\}, \\
R_1 + R_2 &\leq A.
\end{align*}
\]

**Proof:** It is easy to see that one can obtain the result for the case of generating two keys without helpers from Theorem 6 and Theorem 7 by setting $X_3 = \Phi$.

The inner and outer bounds are illustrated in Figure 4. From the figure, we can see that the scheme is sum key rate optimal.

Furthermore, if $A \leq \min\{B, C\}$, the inner and outer bounds in Lemma 10, and hence the full capacity region is characterized. To see this, first, for the outer bound specified in Lemma 10, if $A \leq \min\{B, C\}$, the outer bound is same as

\[
\begin{align*}
R_1 &\leq A, \\
R_2 &\leq A, \\
R_1 + R_2 &\leq A.
\end{align*}
\]

Clearly, the first two bounds are redundant, and hence the outer bound is the same as

\[
R_1 + R_2 \leq A.
\]
Now, we examine the inner bound specified in Lemma 10. If $A \leq \min\{B, C\}$, $P_1$ becomes $(0, A)$, and $P_4$ becomes $(A, 0)$. Using time-sharing between these two points, we obtain the whole region. However, if $A > \min\{B, C\}$, there is a gap between the inner and outer bounds. We will discuss this gap in more details in the next section.

V. Pairwise Independent Network Model

In this section, we consider a special case of the correlation model: pairwise independent network (PIN) model introduced in [18]. In the case of $J + 1$ users considered in this paper, each $X_j$ in the PIN model has $J$ components, such that each component is correlated with one component of another user. In particular, $X_j = [X_{j,0}, \cdots, X_{j,j-1}, X_{j,j+1}, \cdots, X_{j,J+1}]$ with
\( X_{j,k} \) being the component in user \( j \) that is correlated with \( X_{k,j} \), the component in user \( k \) that is correlated with user \( j \). Furthermore the pairs \( (X_{j,k}, X_{k,j}) \) are mutually independent. As the result, in the PIN model,

\[
P_{X_0, \ldots, X_J} = \prod_{0 \leq j < k \leq J} P_{X_{j,k}, X_{k,j}}(x_{j,k}, x_{k,j}).
\] (115)

Figure 5 illustrates the PIN model for three users.

The special structure in the PIN model allows us to obtain better results. In particular, we can fully characterize the capacity region for the general case of generating \( M \) keys with \( J - M \) dedicated helpers.

![Figure 6. The capacity region for PIN model with two users without dedicated helpers.](image_url)

We use the two users without dedicated helpers case as an example to illustrate the main ideas that allow us to get tight results for the PIN model. As discussed in Lemma 10, points \( P_1, P_2, P_3 \) and \( P_4 \) in Figure 6 are achievable. Here, we show that, under PIN model, \( P_5 \) and \( P_6 \) in Figure 6 are also achievable, hence there is no gap between the inner and outer bounds under the PIN model. We discuss point \( P_6 \) in detail. First, we know that

\[
\min\{A, B\} = \min\{I(X_0; X_1 X_2), I(X_1; X_0 X_2)\} = I(X_0; X_1 | X_2) + \min\{I(X_0; X_2), I(X_1; X_2)\}.
\]

As mentioned above, \( P_4 \) is shown to be achievable in [3]. In [3], roughly speaking, to achieve \( R_1 = \min\{A, B\} \), user 2 divides all \( X_2^n \) sequences into

\[
2^n{\max\{H(X_2|X_0), H(X_2|X_1)\} + \epsilon}
\]
bins and sends the bin number as the public discussion information. By combining their local observations with the information sent by user 2, both user 0 and user 1 will be able to decode $X^n_2$, from which both user 0 and user 1 create an additional key (in addition to the key that can be generated from the correlation between $X_0$ and $X_1$ with a rate of $I(X_0; X_1 | X_2)$) with a rate

$$H(X_2) - \max\{H(X_2 | X_0), H(X_2 | X_1)\} = \min\{I(X_0; X_2), I(X_1; X_2)\},$$

which is the contribution of node 2 in achieving $R_1 = \min\{A, B\}$. This scheme is sufficient for achieving $P_4$. However, this scheme is not able to achieve $P_6$ when $\min\{A, B\} = B$. The issue is that by requiring both user 0 and user 1 to fully recover $X^n_2$, user 2 reveals too much information about its observations. With the special pairwise independent structure, one can achieve $R_1 = \min\{A, B\}$ by asking user 2 to reveal less information about $X^n_2$, and user 0 and user 2 recover only part of $X^n_2$. In this way, user 0 and user 2 can use the leftover undisclosed common randomness to generate the key $K_2$ with rate $A - \min\{A, B\}$. In particular, one can use the following simple two-step approach to achieve Point $P_6$.

Figure 7 summarizes the steps of our approach. In the first step, these three users generate local keys using only the correlated component. In particular, we have $X^n_2 = (X^n_{2,0}, X^n_{2,1})$ in the PIN model. User 2 randomly divides all $X^n_{2,0}$ sequences into $2^n(H(X_{2,0} | X_{0,2}) + \epsilon)$ and sends the bin number to user 0. By combining $X^n_{0,2}$ with this bin number, user 0 can recover $X^n_{2,0}$ with a high probability, from which user 2 and user 0 can generate a key $K_{0,2}$ with a rate $I(X_{0,2}; X_{2,0}) - \epsilon$. Similarly, user 2 randomly divides all $X^n_{2,1}$ sequences into $2^n(H(X_{2,1} | X_{1,2}) + \epsilon)$ bins and sends the bin number to user 1. By combining $X^n_{1,2}$ with this bin number, user 1 can recover $X^n_{2,1}$ with a high probability, from which user 2 and user 1 can generate a key $K_{1,2}$ with a rate $I(X_{1,2}; X_{2,1})$. In the same manner, user 0 and user 1 can generate a key $K_{0,1}$ with a rate $I(X_{0,1}; X_{1,0}) - \epsilon$. 

![Figure 7](image-url)
using the correlation \((X_{0,1}^n, X_{1,0}^n)\). Using these local keys, we construct a graph with three nodes and the capacity of the edge between \(i\) and \(j\) is \(n(I(X_{i,j}; X_{j,i}) - \epsilon)\). In the second step, user 0 generates keys \(K_1\) and \(K_2\) and delivers them to user 1 and user 2 using local keys generated in the first step through routing. In particular, user 0 can randomly generate a uniformly distributed key \(K_1 = (K_1^a, K_1^b)\) in which \(K_1^a\) has a rate \(I(X_{0,1}; X_{1,0}) - \epsilon = I(X_0; X_1 | X_2) - \epsilon\) and \(K_1^b\) has a rate \(\min\{I(X_{0,2}; X_{2,0}), I(X_{1,2}; X_{2,1})\} - \epsilon = \min\{I(X_0; X_2), I(X_1; X_2)\} - \epsilon\). User 0 delivers \(K_1^a\), which has \(n(I(X_{0,1}; X_{1,0}) - \epsilon)\) bits, directly to user 1 by encrypting it using \(K_{0,1}\) via the one-time pad scheme. User 1 can then recover \(K_1^a\) using \(K_{0,1}\). User 0 delivers \(K_1^b\), which has \(n(\min\{I(X_0; X_2), I(X_1; X_2)\} - \epsilon)\) bits, to user 1 through user 2. In particular, user 0 uses a part of \(K_{0,2}\) to encrypt \(K_1^b\) using the one-time pad and sends the encrypted message to user 2, which will then decrypt it using \(K_{0,2}\) and then re-encrypt it using \(K_{1,2}\) and sends it to user 1. User 1 can recover \(K_1^b\) using \(K_{1,2}\). Since the rate of \(K_{1,2}\) is \(I(X_0; X_2) - \epsilon = I(X_0; X_2) - \epsilon\) and the rate of \(K_1^b = \min\{I(X_0; X_2), I(X_1; X_2)\} - \epsilon = \min\{I(X_0; X_2), I(X_1; X_2)\} - \epsilon\), part of \(K_{1,2}\) is not needed for delivering \(K_1^b\). This unused part can then used to deliver \(K_2\) to user 2. The leftover rate is \(I(X_{0,2}; X_{2,0}) - \min\{I(X_{0,2}; X_{2,0}), I(X_{1,2}; X_{2,1})\} = A - \min\{A, B\}\), hence \(R_2 = A - \min\{A, B\}\) is achievable.

Essentially, the approach discussed above converts the key generation problem to a two-commodity flows with a single source problem. For this simple example, it is easy to check that by adjusting the rate of keys delivered using different routes, one can not only achieve Point \(P_0\), but also achieve the whole capacity region. This approach can be extended to handle the general case of generating multiple keys with multiple helpers. Coupled with multi-commodity flows with a single source results in the graph theory, we can characterize the full capacity region.

**Theorem 11:** Let \(\mathcal{B} = \{B \subset \mathcal{J} : 0 \in \mathcal{B}^c, B \cap \mathcal{M} \neq \emptyset\}\). The capacity region for generating \(M\) keys with \(J + 1\) users (key \(K_j, j \in \mathcal{M}\) for user \(j\) to be shared with user 0, and users indexed from \(M + 1\) to \(J\) act as helpers) is the union of all rate tuples \((R_1, \cdots, R_M)\) that satisfy the following conditions:

\[
\sum_{m \in \mathcal{M} \cap B} R_m \leq \sum_{(i,j) \in B, j \in \mathcal{B}^c} I(X_{i,j}; X_{j,i}), \forall B \in \mathcal{B}. \tag{116}
\]

**Proof:** Converse: The converse is essentially a cut-set type bound. In particular, for any \(B \in \mathcal{B}\), we create two super nodes \(1_B\) and \(1_{B^c}\). \(1_B\) combines all the observations of nodes \(i \in B\), and \(1_{B^c}\) combines all the observations of nodes \(j \in B^c\). We require these two super nodes to
generate a single key. Since this is a single key generation problem, we know that the key rate capacity is \( [1], [5] \)

\[
C_{1B,1B^c} = I(\{X_i : i \in B\}; \{X_j : j \in B^c\}). \tag{117}
\]

Now, any scheme in our original problem can be used to generate a key for this genie-aided model with a rate \( \sum_{m \in M \cap B} R_m \). Hence,

\[
\sum_{m \in M \cap B} R_m \leq I(\{X_i : i \in B\}; \{X_j : j \in B^c\}) = \sum_{(i,j): i \in B, j \in B^c} I(X_{ij}; X_{ji}). \tag{118}
\]

The last equality is easy to verify by exploiting the pairwise independence structure.

**Achievability:** In the following, we describe a graph-based approach that generalizes the approach discussed above. There are two main steps: 1) graph construction via local key establishment; and 2) key propagation via local keys.

In the first step, we construct a graph \( G_n(V, E) \), in which \( V \) and \( E \) are the set of nodes and edges of the graph respectively. In our graph, \( V \) includes all the nodes in \( J \). Hence, there are \( J + 1 \) nodes in the graph. For each node pair \( (i, j) \), we add an undirected secure link with a link capacity \( e_{ij} = n(I(X_{ij}; X_{ji}) - \epsilon) \). This is done by asking node \( i \) and \( j \) to establish a local key via the existing point-to-point key establishment protocol with the correlated observations \( (X_{nij}, X_{nji}) \) [1]. We use \( K_{ij} \) to denote the value of this local key at node \( i \) and \( K_{ji} \) to denote the value of this key at node \( j \). We have that \( \Pr\{K_{ij} \neq K_{ji}\} \leq \epsilon_1 \). In the following, instead of using both \( K_{ij} \) and \( K_{ji} \) to denote the value of the local key between \( (i, j) \), we will use \( K_{ij} \) to denote both keys with the understanding that there is a small probability that the value of local keys at \( (i, j) \) are different. We use \( F_{ij} \) to denote the public discussion information exchanged in order to establish the local key between \( (i, j) \). From [1], [2], we know that there exists a scheme such that \( I(K_{ij}; F_{ij}) \leq \epsilon_2 \).

In the second step, node 0 randomly generates \( M \) independent keys \( K_m, m = 1, \cdots, M \), each from the set \( \{1, \cdots, 2^{nR_m}\} \) using a uniform distribution. Hence, \( K_m \) has \( nR_m \) bits. Node 0 then delivers each \( K_m \) to node \( m \) using a secure routing approach. More specifically, let \( P_i^m = (0, i_{l,2}, i_{l,3}, \cdots, m) \) be the \( l^{th} \) route between node 0 and node \( m \) in graph \( G_n(V, E) \), and \( Q_i^m \) be the total number of hops in this route. Node 0 divides key \( K_m \) into \( L^m \) non-overlapping parts \( (K_{i1}^m, K_{i2}^m, \cdots, K_{iL^m}^m) \), each having \( W_i^m \) bits, and sends \( K_{i1}^m \) through the \( l^{th} \) route between node 0 and \( m \). In the \( q^{th} \) hop of the \( l^{th} \) route \( (i_{l,q}, i_{l,q+1}) \), node \( i_{l,q} \) encrypts \( K_{i1}^m \) using \( W_i^m \) bits of
the local key $K_{i_l,q,i_{l,q+1}}$. We use $K_{i_l,q,i_{l,q+1}}^{m,l}$ to denote this part of the local key. In this case, node $i_l,q$ uses the one-time pad scheme for encryption, namely node $i_l,q$ broadcasts $K_l^m \oplus K_{i_l,q,i_{l,q+1}}^{m,l}$ over the public channel. Node $i_{l,q+1}$ decrypts $K_l^m$ using the same part of the local key $K_{i_l,q,i_{l,q+1}}^{m,l}$, namely $K_{i_l,q,i_{l,q+1}}^{m,l}$. After that, the node pair $(i_l,q,i_{l,q+1})$ will discard $K_{i_l,q,i_{l,q+1}}^{m,l}$, i.e., $K_{i_l,q,i_{l,q+1}}^{m,l}$, which will not be used again. When we choose routes, we need to make sure that the total amount of key information routed over each edge is smaller than the local key capacity.

Now, we need to show that this approach satisfies the conditions (3) and (4). The independence and uniformness conditions are automatically satisfied since keys $K_m, m = 1, \ldots, M$ are independently generated using the uniform distribution.

We first look at the probability that the value of key $K_m$ recovered at node $m$ is different from $K_m$. The only type of event that may lead to a decoding error at node $m$ is an error during the local key establishment process. More specifically, suppose the link $(i,j)$ is one of the routes used by node $m$, then the event $K_{ij} \neq K_{ji}$ may lead to an error of the key recovered at node $m$. We have

$$\Pr\{K_m \neq \hat{K}_m\} \leq \Pr\{\exists (i,j) \text{ such that } K_{ij} \neq K_{ji}\} \leq \left(\frac{J + 1}{2}\right)\epsilon_1.$$  \hspace{1cm} (119)

Here, we have used the union bound. This probability can be made arbitrarily small.

In the following, we compute the amount of key leakage. Two types of information has been exchanged over the public channel: 1) $\{F_{ij}, 1 \leq i < j \leq J + 1\}$ that are used to establish local keys; 2) $K_l^m \oplus K_{i_l,q,i_{l,q+1}}^{m,l}, 1 \leq m \leq M, 1 \leq l \leq L_m, 1 \leq q \leq Q_m^l\}$ that are used to route
\[ K^m_l, 1 \leq l \leq L^m \] from node 0 to node \( m \). We have

\[
I(K_1, \cdots, K_M; \{F_{ij}, 1 \leq i < j \leq J + 1\}, \{K^m_l \oplus K^m_{l_i,q,i+1}, 1 \leq m \leq M, 1 \leq l \leq L^m, 1 \leq q \leq Q^m_l\})
\]

\[
= I(K_1, \cdots, K_M; \{K^m_l \oplus K^m_{l_i,q,i+1}, 1 \leq m \leq M, 1 \leq l \leq L^m, 1 \leq q \leq Q^m_l\})
\]

\[
\leq I(K_1, \cdots, K_M; \{F_{ij}, 1 \leq i < j \leq J + 1\}) + I(K_1, \cdots, K_M; \{F_{ij}, 1 \leq i < j \leq J + 1\})
\]

\[
= H(\{K^m_l \oplus K^m_{l_i,q,i+1}, 1 \leq m \leq M, 1 \leq l \leq L^m, 1 \leq q \leq Q^m_l\})\{F_{ij}, 1 \leq i < j \leq J + 1\})
\]

\[
\leq H(\{K^m_l, 1 \leq m \leq M, 1 \leq l \leq L^m, 1 \leq q \leq Q^m_l\}) + \sum_{m=1}^{M} \max\{Q^m_l\}L^m(\epsilon + \epsilon_2), \tag{120}
\]

where (a) is due to the uniformity condition. The bound in (120) can be made arbitrarily small as \( n \) increases. This implies that Eve learns negligible amount of information about the generated key \( (K_1, \cdots, K_M) \) from the public discussion and subsequent key routing process.

It is clear that the proposed secure routing key propagation protocol converts the simultaneous key agreement problem into a single source multi-commodity flow over the graph \( G_n(V, E) \) problem [20]. In this equivalent single source multi-commodity flow problem, we have \( M \) commodities that need to be delivered from node 0 to node \( m \in \mathcal{M} \) with the constraint that the total amount of flows on each link cannot exceed the flow capacity, namely the local key rate of each link. Furthermore, each commodity is demanded by only one user. Maximizing the achievable key rates using this approach is the same as maximizing the rates of these \( M \) flows by carefully selecting the routes and the amount of flow over each route. From the celebrated max-flow min-cut theorem [22], we know that for a such single source multi-commodity flow problem, as long as the amount of flows satisfies cut conditions, there exists a fractional routing scheme from user 0 to the \( \mathcal{M} \) for these flows. Regarding the graph \( G_n(V, E) \) constructed in our scheme, for any cut that divides \( V \) into \( B \) and \( B^c \), the cut condition implies

\[
\sum_{m \in B \cap \mathcal{M}} \log_2 |K_m| \leq \sum_{(i,j):i \in B,j \in B^c} n(I(X_{i,j}; X_{j,i}) - \epsilon), \tag{121}
\]

which is exactly the same as (116). Although the number of key bits in our problem must be an
integer, rounding the fractional solution to an integer solution will not affect the key rate. Thus, our graph based scheme achieves the whole capacity for this general case.

VI. NUMERICAL EXAMPLE

In this section, we use an example to illustrate various regions derived in the previous sections. In this example, we consider a binary PIN model. Each component is binary with equal probability of being 0 or 1. The components of the same user are independent with each other, while \( \Pr\{X_{j_1,j_2} \neq X_{j_2,j_1}\} = \rho_{j_1,j_2} = \rho_{j_2,j_1} \leq 1/2 \).

We first consider the case of generating two keys without dedicated helpers. Using Theorem 11, straightforward calculations show that the capacity region of two keys without a helper is

\[
R_2 \leq 2 - h_b(\rho_{0,2}) - h_b(\max\{\rho_{0,1}, \rho_{1,2}\}),
R_1 + R_2 \leq 2 - h_b(\rho_{0,2}) - h_b(\rho_{0,1}),
R_1 \leq 2 - h_b(\rho_{0,1}) - h_b(\max\{\rho_{0,2}, \rho_{1,2}\}).
\]

(122)

Now, for the case of generating \( J \) keys without helpers, it is easy to calculate that the sum key rate capacity is

\[
C_{\text{sum}} = I(X_0; X_1, \cdots, X_J) = J - \sum_{j=1}^{J} h_b(\rho_{0,j}).
\]

(123)
In the following, we evaluate the rate region for the capacity of generating two keys with one helper. We denote

$$a_1 = 4 - h_b(\rho_{0,1}) - h_b(\rho_{2,3}) - \max\{h_b(\rho_{0,2}) + h_b(\rho_{1,3}), h_b(\rho_{0,3}) + h_b(\rho_{1,2})\},$$  \hspace{1cm} (124) \\
a_2 = 3 - \sum_{j=1}^{3} h_b(\rho_{0,j}), \hspace{1cm} (125) \\
a_3 = 3 - h_b(\rho_{0,1}) - h_b(\rho_{1,2}) - h_b(\rho_{1,3}), \hspace{1cm} (126) \\
a_4 = 4 - h_b(\rho_{0,2}) - h_b(\rho_{1,3}) - \max\{h_b(\rho_{0,3}) + h_b(\rho_{1,2}), h_b(\rho_{0,1}) + h_b(\rho_{2,3})\}, \hspace{1cm} (127) \\
a_5 = 3 - h_b(\rho_{0,3}) - h_b(\rho_{1,2}) - h_b(\rho_{2,3}). \hspace{1cm} (128)$$

Specializing Theorem 11 to this binary PIN model with one helper, one can also verify that the capacity region can be written as

$$R_1 \leq \min\{a_1, a_2, a_3\}, \hspace{1cm} (129)$$

$$R_2 \leq \min\{a_2, a_4, a_5\}, \hspace{1cm} (130)$$

$$R_1 + R_2 \leq \min\{a_2, 4 - h_b(\rho_{0,1}) - h_b(\rho_{2,3}) - h_b(\rho_{0,2}) - h_b(\rho_{1,3}) - h_b(\rho_{1,2})\}. \hspace{1cm} (131)$$

Figures 8 - 10 compare the regions for the cases with and without a helper under different values of parameters. As we can see from the figure, having a helper can substantially increase the key rate region. Furthermore, depending on the value of the parameters, the shapes of the regions vary.
We have formulated the problem of simultaneously establishing multiple keys, one for each user in a set of users. This scenario arises when there are multiple users wishing to communicate securely with a base-station. For the case of generating multiple keys with no dedicated helpers, we have developed a scheme that achieves the sum key rate capacity. We have also extended the study to the scenario in which there are several dedicated helpers whose sole purpose is to assist the key generation process for other users. We have developed a simple achievable scheme and derived an outer bound for the general case. We have characterized the conditions under which the developed scheme achieves the full capacity regions and conditions under which the scheme is sum-rate optimal. We have also considered the PIN model, in which we have fully characterized the capacity region for the general case of generating multiple keys with multiple dedicated helpers. We have provided some numerical examples to illustrate the results derived in this paper.

There are several interesting directions for the future work. First, it will be interesting to extend the study to a more general network as shown in Figure 1 (b). We have made some initial progress along this line under the PIN model [17]. Second, it is important to study the scenario in which each key is secured from the helpers. Third, it is of interest to study the scenario in which Eve has side-information. Finally, it is also important to study the scenario with active attackers.
APPENDIX A
CONDITIONS FOR SOURCE CODING WITH SIDE INFORMATION

For any subset of users $S \subset \{1, \cdots, J\}$, let $s_i, i = 1, \cdots, |S|$ be the indices of users in the set $S$. Without loss of generality, we assume $s_i < s_i'$ if $i < i'$. For this set of value of $b_j$ in (14), we have

$$H(X_S|X_{Sc}, X_0) = \sum_{i=|S|}^1 H(X_{s_i}|X_{s_i[S]}, \cdots, X_{s_i+1}, X_0)$$

$$\leq \sum_{i=|S|}^1 H(X_{s_i}|X_{s_i[S]}, \cdots, X_{s_i+1}, X_0) \cap \{X_0, X_{[s_i+1, J]}\}$$

$$= \sum_{i=|S|}^1 H(X_{s_i}|X_0, X_{[s_i+1, J]})$$

$$\leq \sum_{i=|S|}^1 H(X_{s_i}|X_0, X_{[s_i+1, J]}) + \epsilon$$

$$= \frac{1}{n} \sum_{i \in S} \log b_i. \quad (132)$$

The condition (132) implies that the rates in (14) satisfy the conditions for successful source recovery in source coding with side information [23]. Hence, we know that user $X_0$ can obtain an estimate $(\hat{X}_n^1, \cdots, \hat{X}_n^J)$ from $(x_0^n, f_{X_1}(X_1^n), \cdots, f_{X_J}(X_J^n))$ such that

$$\Pr\{(\hat{X}_1^n, \cdots, \hat{X}_J^n) \neq (X_1^n, \cdots, X_J^n)\} \leq \epsilon. \quad (133)$$

APPENDIX B
PROOF OF THEOREM 7

We first prove that following lemma that is applicable for the general case with multiple helper nodes. More specifically, users indexed from 3 to $J$ are helpers. Before proceeding, we give several definitions. Let $B = B_I \cup B_{II} \cup B_{III} \cup B_{IV}$ with

$$B_I = \{B \subset J : \{0, 1\} \text{ crosses } B \text{ and } \{0, 2\} \text{ crosses } B, \text{ or } 0 \in B^c\}, \quad (134)$$

$$B_{II} = \{B \subset J : \{0, 1\} \subset B \text{ and } 2 \in B^c\}, \quad (135)$$

$$B_{III} = \{B \subset J : \{0, 2\} \subset B \text{ and } 1 \in B^c\}, \quad (136)$$

$$B_{IV} = \{B \subset J : \{0, 1, 2\} \subset B\}. \quad (137)$$
and $B_j$ be the set of subsets that contain user $j$. Here $\{i, j\}$ crosses $B$ means $\{i, j\} \cap B \neq \emptyset$ and $\{i, j\} \cap B^c \neq \emptyset$. Let $\Lambda$ be the set of all collections $\lambda = \{\lambda_B : B \in \mathcal{B}\}$ of weights $0 \leq \lambda_B \leq 1$ satisfying
\[
\sum_{B \in B_j} \lambda_B = 1 \text{ for all } j \in \mathcal{J}.
\] (138)

**Lemma 12:** For any $\lambda \in \Lambda$,
\[
\left(1 - \sum_{B \in B_{I_1} \cup B_{I_2}} \lambda_B\right) R_1 + \left(1 - \sum_{B \in B_{I_3} \cup B_{I_4}} \lambda_B\right) R_2 \leq H(X_\mathcal{J}) - \sum \lambda_B H(X_B|X_B^c). \tag{139}
\]

**Proof:** The proof is an extension of the proof of Theorem 1 in [2].

\[
H(X^n_{\mathcal{J}}) = H(F, K_1, K_2, X^n_0, \cdots, X^n_j)
= \sum_{v=1}^{r(J+1)} H(F_v|F_{[1,v-1]}) + H(K_1, K_2|F) + \sum_{j=0}^{J} H(X^n_j|F, K_1, K_2, X^n_{[0,j-1]}).
\]

Setting
\[
S_j' = \frac{1}{n} \sum_{v:j = v \mod (J+1)} H(F_v|F_{[1,v-1]}) + \frac{1}{n} H(X^n_j|F, K_1, K_2, X^n_{[0,j-1]}), \tag{140}
\]
we have
\[
H(K_1, K_2|F) = H(X^n_{\mathcal{J}}) - \sum_{j=0}^{J} S_j'. \tag{141}
\]

In addition, we set
\[
S_j = S_j' + \frac{\epsilon \log |K_1||K_2| + 1}{n}. \tag{142}
\]

For any set $B \subset \mathcal{J}$
\[
H(X^n_B|X^n_{B^c}) \tag{143}
= H(F, K_1, K_2, X^n_B|X^n_{B^c})
= \sum_{v=1}^{r(J+1)} H(F_v|F_{[1,v-1]}, X^n_{B^c}) + H(K_1, K_2|F, X^n_{B^c})
+ \sum_{j \in B} H(X^n_j|F, K_1, K_2, X^n_{[0,j-1]}, X^n_{B^c \cap [j+1,J]}). \tag{144}
\]

From here, depending on the elements in the set $B$, we can derive four types of inequalities.
1) If $B \in B_I$, then based on Fano’s inequality,

$$H(K_1, K_2|F, X_{B^c}^n) \leq \epsilon \log |\mathcal{K}_1||\mathcal{K}_2| + 1. \quad (145)$$

Plugging this back into (144) gives

$$H(X_B|X_{B^c}) \leq \sum_{j \in B} S_j. \quad (146)$$

2) If $B \in B_{II}$,

$$H(K_1, K_2|F, X_{B^c}^n) = H(K_2|F, X_{B^c}^n) + H(K_1|F, X_{B^c}^n, K_2) \leq \epsilon \log |\mathcal{K}_1||\mathcal{K}_2| + 1 + H(K_1). \quad (147)$$

Here, we have the inequality since $2 \in B^c$, which implies that one can recover $K_2$ from $(F, X_{B^c}^n)$. Plugging this back into (144) gives

$$H(X_B|X_{B^c}) \leq \sum_{j \in B} S_j + \frac{1}{n} H(K_1). \quad (148)$$

3) If $B \in B_{III}$, following the same steps as above, we have

$$H(X_B|X_{B^c}) \leq \sum_{j \in B} S_j + \frac{1}{n} H(K_2), \quad (149)$$

4) If $B \in B_{IV}$, we have

$$H(X_B|X_{B^c}) \leq \sum_{j \in B} S_j + \frac{1}{n} H(K_1) + \frac{1}{n} H(K_2), \quad (150)$$

Since, we require $K_1$ and $K_2$ to be independent, we have

$$R_1 + R_2 = \frac{1}{n}(H(K_1) + H(K_2)) \overset{(a)}{\leq} \frac{1}{n} H(K_1, K_2|F) + \epsilon_n \overset{(b)}{\leq} H(X_{\mathcal{F}}) - \sum_{j=0}^{J} S_j + \epsilon_n$$

$$= H(X_{\mathcal{F}}) - \sum_{j=0}^{J} S_j + \frac{\epsilon \log |\mathcal{K}_1||\mathcal{K}_2| + 1}{n} + \epsilon_n \quad (151)$$

Here, (a) is due to the secrecy constraint, and (b) is due to (141).
Now, for any $\lambda \in \Lambda$, we have
\[
\sum_{B \in \mathcal{B}_i} \lambda_B H(X_B|X_{B^c}) = \sum_{B \in \mathcal{B}_i} \lambda_B H(X_B|X_{B^c}) + \sum_{B \in \mathcal{B}_{II}} \lambda_B H(X_B|X_{B^c}) + \sum_{B \in \mathcal{B}_{III}} \lambda_B H(X_B|X_{B^c}) + \sum_{B \in \mathcal{B}_{IV}} \lambda_B H(X_B|X_{B^c})
\]
\[
\leq \sum_{B \in \mathcal{B}_i} \lambda_B \sum_{j \in B} S_j + \sum_{B \in \mathcal{B}_{II}} \lambda_B \left( \sum_{j \in B} S_j + \frac{1}{n} H(K_1) \right) + \sum_{B \in \mathcal{B}_{III}} \lambda_B \left( \sum_{j \in B} S_j + \frac{1}{n} H(K_2) \right)
\]
\[
+ \sum_{B \in \mathcal{B}_{IV}} \lambda_B \left( \sum_{j \in B} S_j + \frac{1}{n} H(K_1) + \frac{1}{n} H(K_2) \right)
\]
\[
= \sum_{j \in \mathcal{J}} \sum_{B \subseteq B_j} \lambda_B S_j + \frac{1}{n} \sum_{B \in \mathcal{B}_{II} \cup \mathcal{B}_{IV}} \lambda_B H(K_1) + \frac{1}{n} \sum_{B \in \mathcal{B}_{III} \cup \mathcal{B}_{IV}} \lambda_B H(K_2)
\]
\[
= \sum_{j \in \mathcal{J}} S_j + \frac{1}{n} \sum_{B \subseteq B_j} \lambda_B H(K_1) + \frac{1}{n} \sum_{B \in \mathcal{B}_{II} \cup \mathcal{B}_{IV}} \lambda_B H(K_2), \quad (152)
\]

since for each $j$, $\sum_{B \subseteq B_j} \lambda_B = 1$ for any $\lambda \in \Lambda$.

Plugging (152) into (151), we have the desired result.

Specializing Lemma 12 to the single helper case, we have the following inequalities:

\[
H(X_0|X_1X_2X_3) \leq S_0, \quad (153)
\]
\[
H(X_1X_2X_3|X_0) \leq S_1 + S_2 + S_3, \quad (154)
\]
\[
H(X_0X_3|X_1X_2) \leq S_0 + S_3, \quad (155)
\]
\[
H(X_1X_2|X_0X_3) \leq S_1 + S_2, \quad (156)
\]
\[
H(X_0X_1|X_2X_3) \leq S_0 + S_1 + R_1, \quad (157)
\]
\[
H(X_2X_3|X_0X_1) \leq S_2 + S_3, \quad (158)
\]
\[
H(X_0X_1X_2|X_3) \leq S_0 + S_1 + S_2 + R_1 + R_2, \quad (159)
\]
\[
H(X_3|X_0X_1X_2) \leq S_3, \quad (160)
\]
\[
H(X_0X_1X_3|X_2) \leq S_0 + S_1 + S_3 + R_1, \quad (161)
\]
\[
H(X_2|X_0X_1X_3) \leq S_2, \quad (162)
\]
\begin{align}
H(X_0X_2|X_1X_3) & \leq S_0 + S_2 + R_2, \quad (163) \\
H(X_1X_3|X_0X_2) & \leq S_1 + S_3, \quad (164) \\
H(X_0X_2X_3|X_1) & \leq S_0 + S_2 + S_3 + R_2, \quad (165) \\
H(X_1|X_0X_2X_3) & \leq S_1. \quad (166)
\end{align}

The bounds on \( R_1 \) can be obtained using type III inequalities, \( R_2 \) via type II inequalities and \( R_1 + R_2 \) using type I inequalities. These can also be obtained using cut-set bounds.

In the following, we show how to get the bound on \( 2R_1 + R_2 \). By assigning the weight \( \lambda = 1/2 \) for (153), (156), (158), and (161), and adding them up, we have

\[
\frac{1}{2}(H(X_0|X_{0}) + H(X_{1,2}|X_{0,3}) + H(X_{2,3}|X_{0,1}) + H(X_{2}|X_{2})) \leq \sum S_i + \frac{1}{2}R_1 \quad (167)
\]

Plug this in (151), and we have that

\[
R_1 + 2R_2 \leq 2H(X_J) - (H(X_0|X_{0}) + H(X_{1,2}|X_{0,3}) + H(X_{2,3}|X_{0,1}) + H(X_{2}|X_{2})) \quad (168)
\]

The other bound on \( R_1 + 2R_2 \) can be obtained by assigning weight \( \lambda = 1/2 \) for (154), (155), (157), and (162). Similarly, the bounds on \( 2R_1 + R_1 \) can be obtained by assigning weight \( \lambda = 1/2 \) for 1) (154), (155), (163), and (166); or 2) (153), (156), (164), and (165) respectively. We note that there are several other possible weight assignments \( \lambda \), but after checking them carefully, we found the bounds obtained using those assignments are redundant.

**References**


