On the Optimality of Secret Key Agreement via Omniscience

Chung Chan, Manuj Mukherjee, Navin Kashyap, Senior Member, IEEE, and Qiaoqiao Zhou

Abstract—For the multiterminal secret key agreement problem under a private source model, it is known that the maximum key rate, i.e., the secrecy capacity, can be achieved through communication for omniscience, but the omniscience strategy can be strictly suboptimal in terms of minimizing the public discussion rate. While a single-letter characterization is not known for the minimum discussion rate needed for achieving the secrecy capacity, we derive single-letter lower bounds that yield some simple conditions for omniscience to be discussion-rate optimal. These conditions turn out to be enough to deduce the optimality of omniscience for a large class of sources, including the hypergraphical sources. We also extend our results to more general class of multiterminal sources with helpers and silent users.

Index Terms—Secret key agreement, omniscience, multivariate mutual information, Wyner common information, Gács-Körner common information.

I. INTRODUCTION

We consider the secret key agreement problem of [1], possibly with trusted and untrusted helpers, as well as silent users as in [2]. Two or more users want to agree on a secret key after observing some discrete memoryless correlated private sources that take values from finite alphabet sets. The users are allowed to discuss (possibly interactively) with other users publicly over a noiseless authenticated broadcast channel. After the discussion, each active user (who is not a helper) attempts to compute a common secret key that is asymptotically uniformly random and independent of the public discussion as well as the private sources of the untrusted helpers. The maximum achievable key rate is called the secrecy capacity $C_S$, and the minimum public discussion rate required to achieve the capacity is called the communication complexity $R_S$. While $C_S$ was characterized in [1], a single-letter characterization for $R_S$ remains open, and is the main focus of this work.

For the general source model with possibly trusted helpers, it was shown in [1] that $R_S$ can be upper bounded by the smallest rate $R_{CO}$ of communication for omniscience (CO), the state where every active user can asymptotically recover the entire private source. More precisely, the proposed capacity-achieving scheme is through omniscience, i.e., by having users communicate in public until every user recovers the entire private source and then extract a common secret key as a function of the recovered source that is asymptotically independent of the public discussion. While this omniscience strategy was shown to be capacity-achieving, it was also pointed out in [1] to be suboptimal in the sense that strict inequality $R_S < R_{CO}$ is possible.

For the general source model with two users but no helpers, there is a multi-letter characterization of $R_S$ in [3]. An example was also given where non-interactive discussion, i.e., the usual independent source coding scheme over a source network [4], was shown to be suboptimal. When the number of discussion rounds is bounded, such a characterization becomes a single-letter expression. Mukherjee et al. [5] extended the framework of [3] to the multiterminal case and obtained a lower bound on $R_S$. The lower bound is a multi-letter expression even when the number of rounds is bounded. A special hypergraphical private source model [6] was also considered in [7] in the multi-user case but without helpers, and $R_S$ was characterized when the discussion is non-asymptotic (one-shot) and restricted to be linear functions of the sources over a finite field. However, the expression was NP-hard to compute, and it was shown to be a loose upper bound for $R_S$ in the asymptotic model [7].

In this work, we consider a different question that turns out to be easier to address than the problem of characterizing $R_S$: When is omniscience optimal for achieving secrecy capacity, i.e., when is $R_S = R_{CO}$? This question was raised in [8] in the no-helper case, and a sufficient condition for the optimality of omniscience was given in the special case of the pairwise independent network (PIN) model defined in [9] and [10]. The sufficient condition was later shown to be necessary in [5]. However, the result does not apply to more general source models beyond PIN, such as the hypergraphical model. Moreover, the problem formulation in [5] precludes additional randomization in the public discussion; it was conjectured (but not proved) there that randomization does not affect $R_S$.

In this work, we overcome the above weaknesses through the following contributions. Our main focus remains the gen-
eral source model without helpers and silent users, for which we single-letterize the lower bound on $R_S$ studied in [5], with private randomization allowed at the terminals. This single-letterization then allows us to derive a simple condition to test whether $R_S = R_{CO}$. In fact, we show using the idea of *decremental secret key agreement* [11], [12] that this condition turns out to be necessary to ensure $R_S = R_{CO}$ for the hypergraphical source. However, the necessity of this condition no longer extends to more general sources, which we illustrate using an example. We then look at multiterminal sources with helpers, both trusted and untrusted, and silent users. We show that secret key capacity can still be achieved in this scenario through a communication for omniscience, thereby unifying the results of Csiszár and Narayan [1] and Gohari and Anantharam [2]. We would like to point out that our result is not a simple juxtaposition of the results in [1] and [2]. According to [1], every untrusted helper is supposed to reveal its entire source. However, our scheme requires the untrusted helpers to communicate in such a way that every active user can recover the source of all the untrusted users together. Therefore, this scheme does not necessitate each untrusted helper to reveal its source entirely, thereby lowering the communication rates. In fact, we demonstrate using examples that the minimum rate of communication for omniscience can be strictly lower than the one obtained through a simple juxtaposition of the schemes in [1] and [2]. We note that like the case without helpers and silent users, the lower bound to $R_S$ and the condition to check whether $R_S = R_{CO}$ holds for the setting involving helpers and silent users with added technicalities. Specifically for the case with silent users and without untrusted helpers we are able to strengthen our lower bounds on $R_S$ through a new characterization of the secret key capacity. The lower bounds can be further strengthened when restricted to hypergraphical sources, and we are able to derive a necessary and sufficient condition for $R_S = R_{CO}$ to hold. Finally, we illustrate a class of techniques, which we call change of scenario, to obtain lower and upper bounds on $R_S$ and whenever possible to translate them to conditions for checking whether $R_S = R_{CO}$.

The paper is organized as follows. We begin by introducing the multiteminal source model without helpers and silent users in Section II, and review some of the known results. Single-letter lower bounds to $R_S$ and a condition for checking whether $R_S = R_{CO}$ is included in Section III. Extensions of our results to the case with helpers and silent users are provided in Section IV. Section V summarizes the results in this paper and highlights the open problems. Some of the more technical proofs are presented in the appendices.

II. PROBLEM FORMULATION

In this section we shall introduce the problem of secret key generation in the multiterminal source model. We shall restrict our attention to the scenario without helpers and silent users. The case involving helpers and silent users is treated in Section IV.

Before proceeding, a word on the notation. We use $\mathbb{N}$ and $\mathbb{R}$ to denote the set of natural numbers and real numbers respectively. For any $m \in \mathbb{N}$, we define the notation $[m] := \{1, 2, \ldots, m\}$. For any finite set $A$, we shall use $\mathbb{R}^A$ to denote the set $\mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$. Given any vector $r_A = (r_1, r_2, \ldots, r_{|A|})$, and any $B \subseteq A$, we define $r_B := (r_i \mid i \in B)$ and $r(B) := \sum_{i \in B} r_i$.

Let $V$ be the ordered finite set of all users, where $|V| \geq 2$. Unless stated otherwise, we assume $V = [|V|]$. The users have access to a private (discrete memoryless multiple) source denoted by the random vector

$$Z_V := (Z_i \mid i \in V) \sim P_{Z_V}$$

taking values from (2.1a)

$$Z_V := \prod_{i \in V} Z_i,$$  \hspace{1cm} (2.1b)

which is assumed to be finite. Note that, for notational convenience, we use capital letter in sans serif font for random variables and the same capital letter in the usual math italic font for the alphabet sets. $P_{Z_V}$ denotes the joint distribution of $Z_V$’s.

The users discuss in public until they can recover a secret key of their choice that is secured against a wiretapper who can listen to the public discussion. The protocol can be divided into the following phases for ease of exposition:

Secret key agreement protocol

- **Private observation**: Each user $i \in V$ observes an i.i.d. sequence

$$Z^n_i := (Z_{it} \mid t \in [n]) = (Z_{i1}, \ldots, Z_{in})$$

of its private source $Z_i$ for some block length $n$.

- **Private randomization**: Each user $i \in V$ generates a random variable $U_i$ independent of the private source, i.e.,

$$H(U_i | Z^n_i) = \sum_{i \in V} H(U_i).$$  \hspace{1cm} (2.2)

For convenience, we let

$$\tilde{Z}_i := (U_i, Z^n_i) \quad \forall i \in V$$

be the entire private observation of user $i \in V$.

- **Public discussion**: Using a public authenticated noiseless channel, the users broadcast some messages in a round-robin fashion interactively for a finite number of rounds. More precisely, at times $t = 1, \ldots, r$ for some positive integer $r$, the user $i \in V$ broadcasts to everyone a function of its accumulated observations, denoted as

$$F_{it} := f_{it}(\tilde{Z}_i, \tilde{F}_{it})$$

where

$$\tilde{F}_{it} := (F_{[i-1]t}, F^{-1}_{V})$$

which includes the previous messages $F_{[i-1]t} := (F_{jt} \mid j < i)$ broadcast in the same round and the messages $F_{V}^{-1} := (F_{V(t) \mid \tau < t} = (F_{it} \mid i \in V, \tau < t)$ broadcast in previous rounds. Note that, unless otherwise stated, we assumed without loss of generality that the discussion in each round is in the
The secrecy capacity is then defined as
\[
C_S := \sup_{n \to \infty} \lim_{n \to \infty} \inf \log |K| \quad (2.8)
\]
where the supremum is taken over all key rates achievable with any sequence (in \( n \)) of choices of other parameters respecting the constraints on private randomization (2.2), interactive public discussion (2.4) as well as recoverability (2.6) and secrecy (2.7) of the secret key. A \( C_S \)-achieving scheme corresponds to a sequence of choices with achievable key rate equal to the capacity. If the supremum in (2.8) and the constraints (2.6) and (2.7) can be achieved for a finite \( n \), the capacity is said to be achievable non-asymptotically.

In [1], an explicit \( C_S \)-achieving scheme was derived. This scheme involves a communication for omniscience, i.e., a communication using which every user is able to recover the private source of all other users. To be precise, we call \( F \) a communication for omniscience if there exist functions \( \phi_i(\mathbf{Z}_i, F) \), \( i \in V \), satisfying
\[
\lim_{n \to \infty} \Pr \left( \exists i \in V, \mathbf{Z}_i^r \neq \phi_i(\mathbf{Z}_i, F) \right) = 0.
\]

We denote by \( R_{CO} \) the minimum rate of communication for omniscience. It was further shown in [1] that the secret key capacity \( C_S \) is given by
\[
C_S = H(\mathbf{Z}_V) - R_{CO}. \quad (2.9)
\]

The authors also showed that
\[
R_{CO} = \min_{r_V \in \mathcal{R}(\mathbf{Z}_V)} r(\mathbf{V}), \quad (2.10)
\]
where
\[
\mathcal{R}(\mathbf{Z}_V) = \{ r_V \in \mathbb{R}^{|V|} \mid r(B) \geq H(\mathbf{Z}_B|\mathbf{Z}_{V \setminus B}), \forall B \subseteq V \}. \quad (2.11)
\]

The communication complexity is the minimum public discussion rate required to achieve the secrecy capacity, i.e.,
\[
R_S := \inf \lim_{n \to \infty} \sup \log |F|, \quad (2.12)
\]
where \( F \) denotes the finite alphabet set of possible values of \( F \) and the infimum is taken over all the discussion rates of \( C_S \)-achieving schemes.

The fact that communication for omniscience is a \( C_S \)-achieving protocol leads to the upper bound \( R_S \leq R_{CO} \). In fact, the bound is easily computable since the expression for \( R_{CO} \) in (2.10) was argued to be solvable in polynomial time\(^1\) with respect to the size of the network [13], [14].

The upper bound can be loose, as in the following example. Example 1: Let \( X_0, X_1 \) and \( J \) be uniformly random and independent bits. Suppose users 1 and 2 observe the private sources
\[
Z_1 := (X_0, X_1) \quad \text{and} \quad Z_2 := (X_J, J)
\]
respectively, where \( X_J \) is equal to \( X_0 \) if \( J = 0 \), and equal to \( X_1 \) otherwise. A secret key agreement scheme with block length \( n = 1 \) is to have
\[
F := F_2 = J \quad \text{and} \quad K := Z_J,
\]
i.e., have user 2 reveal \( J \) in public so that both users can compute and use \( X_J \) as the secret key, which can be shown to be independent of \( F \) as desired. This is capacity-achieving because the secrecy capacity in the two-user case is the mutual information [1]
\[
C_S = I(Z_1 \wedge Z_2) = 1
\]
and so the communication complexity \( R_S \) is at most \( H(J) = 1 \). Note that omniscience has not been attained because \( H(Z_1|Z_2) > 0 \) (and so user 2 cannot recover \( Z_{1-J} \) unless user 1 also communicates). More precisely, from [1], the minimum rate of communication for omniscience is
\[
R_{CO} = H(Z_1|Z_2) + H(Z_2|Z_1) = 2 > 1 \geq R_S.
\]

In particular, to achieve omniscience, user 1 needs to discuss at rate at least \( H(Z_1|Z_2) \) while user 2 needs to discuss at rate at least \( H(Z_2|Z_1) \); hence the \( R_{CO} \) formula above. □

We say that omniscience is optimal for secret key agreement if the bound is tight, i.e., \( R_S = R_{CO} \), in which case \( R_S \) has a single-letter characterization given by \( R_{CO} \). With only two users, the following is a simple condition for omniscience to be optimal.

Proposition 2: For the two-user case, \( R_S = R_{CO} \) iff \( R_S = 0 \), i.e., \( H(Z_1|Z_2) = H(Z_2|Z_1) = 0 \) where \( Z_i \) is the private source observed by user \( i \in \{1, 2\} \). □

Proof: The “if” case is trivial and follows from the bound \( R_S \leq R_{CO} \). To prove the “only if” case, note that the capacity-achieving scheme of [15] and [16] has a discussion rate of \( \min(h(Z_1|Z_2), h(Z_2|Z_1)) \in \{R_S, R_{CO}\} \). \( R_S = R_{CO} \) implies
\[\text{This is assuming that the entropy function } B \mapsto H(Z_B) \text{ for each } B \subseteq V \text{ can be evaluated in polynomial time.}\]
that the minimum is $R_{\text{CO}} = H(Z_1 | Z_2) + H(Z_2 | Z_1)$ [1], which happens iff $H(Z_1 | Z_2) = H(Z_2 | Z_1) = 0$, or equivalently, $R_{\text{CO}} = 0$.

Our goal is to discover general classes of sources with three or more users where omniscience is or is not optimal, i.e., the sufficient or necessary conditions for the optimality of omniscience. Consider the following example.

Example 3: Suppose user 3 observes the private source

$$Z_3 := Z_1 \oplus Z_2,$$

(2.14)

which is the XOR of two uniformly random and independent bits $Z_1$ and $Z_2$ observed by users 1 and 2 respectively.

In the no-helper case, a secret key agreement scheme is to have each user $i \in \{1, 2, 3\}$ observe $n = 2$ i.i.d. samples, $Z_{i1}$ and $Z_{i2}$, of its private source, and then choose

$$F := (F_1, F_2, F_3) = (Z_{11} \oplus Z_{12}, Z_{22}, Z_{31})$$

and $K := Z_{11}$.

It can be shown that $K$ is independent of $(F_1, F_2, F_3)$ and therefore secure. User 1 can recover the key trivially, while users 2 and 3 can recover it from their observations and the public discussion by computing respectively

$$F_3 \oplus Z_{21} = K$$

and

$$F_1 \oplus F_2 \oplus Z_{32} = K$$

by (2.14). This is capacity-achieving because the secrecy capacity is upper bounded by [1, eq. (26)] as

$$C_S \leq \frac{1}{2} \left[ \sum_{i=1}^{3} H(Z_i) - H(Z_1, Z_2, Z_3) \right] = \frac{1}{2},$$

which is achieved by the current scheme. Omniscience is also attained because $H(K, F) = 4$, which is the randomness of the entire source sequence $(Z_{11}, Z_{22}, Z_{31})$. Since every user can observe $F$ and recover $K$, they can also recover the entire source sequence.

Our result will be able to show that $R_S = R_{\text{CO}}$ for this example. In particular, we are able to specialize/strengthen our results to the hypergraphical source model which is discussed next.

The hypergraphical source [6], [7], [17] is a special case of the multiterminal source model.

Definition 4 ([6, Definition 2.4]): $Z_V$ is a hypergraphical source with respect to a hypergraph $(V, E, \xi)$ with edge function $\xi : E \to 2^n \setminus \{\emptyset\}$ (which maps from an edge label in $E$ to a non-empty subset of $V$) iff

$$Z_i = (X_e \mid e \in E, i \in \xi(e)) \quad \forall i \in V.$$

(3.15)

for some independent (hyper-)edge variables $X_e$ for $e \in E$ with $H(X_e) > 0$.

The above source model also covers the PIN model in [9] and [10] as a special case:

Definition 5 [10]: $Z_V$ is a PIN if it is hypergraphical with respect to a graph $(V, E, \xi)$ with edge function $\xi : E \to \binom{V}{2}$ (no self-loops).

## III. MAIN RESULTS

This section presents the main results of this paper. We will begin by introducing the notions of multivariate mutual information and Wyner common information, which will be needed to state our results. Next we shall single-letterize the lower bound $R_S$ stated in [5], using which we will derive a sufficient condition to identify sources where $R_S = R_{\text{CO}}$. We will then show that this sufficient condition is also necessary in the case of hypergraphical sources, and also identify non-hypergraphical sources where the condition is not necessary.

### A. Preliminaries on MMI, Fundamental Partition and Wyner Common Information

To study the tightness of the $R_{\text{CO}}$ upper bound, we will make use of the following (conditional) multivariate mutual information (MMI) measure and its properties studied in [18]: For a finite set $U$ and a random vector $(Z'_U, W)$,

$$I(Z'_U \mid W) := \min_{P \in \Pi(U)} I_{P}(Z'_U \mid W),$$

(3.1a)

$$I_{P}(Z'_U \mid W) := \frac{1}{|P|} D \left( P_{Z'_U|W} \mid \prod_{C \in P} P_{Z_C \mid W} P_W \right)$$

$$:= \frac{1}{|P|} \sum_{C \in P} H(Z'_U \mid W) - H(Z'_U \mid W),$$

(3.1b)

where $\Pi(U)$ is the collection of partitions of $U$ into at least two non-empty disjoint parts, and $D(\cdot \mid \cdot)$ is the conditional Kullback–Leibler divergence. We also define the unconditional MMI measures $I(Z'_U)$ and $I_{P}(Z'_U)$ by dropping the conditioning on $W$ throughout (3.1).

The MMI appeared as an upper bound on the secrecy capacity in [1, eq. (25)] in the special case without helpers. In [19], the bound [1, eq. (25)] was shown to be loose in the more general case with helpers but identified to be tight in the no-helper case and therefore proposed as a measure of mutual information among multiple random variables:

Proposition 6 ([6, Th. 1.1]): For the source $Z_V$, we have

$$C_S = I(Z'_V).$$

The proof uses the submodularity [20] of the entropy function $B \mapsto H(Z'_B \mid W)$ for $B \subseteq U$ (a class of Shannon-type inequalities [21], [22]) to show that the linear-programming characterization of $C_S$ in [1] is equal to the MMI. A simple proof using the Dilworth truncation was given in [18]. Like Shannon’s mutual information, the MMI has various fundamental-information-theoretic properties including the data processing inequality [18].

Denote the set of all optimal partitions to (3.1a) as

$$\Pi^*(Z_U \mid W) := \{ P \in \Pi'(U) \mid I_{P}(Z'_U \mid W) = I(Z'_U \mid W) \}.$$  \hspace{1em} (3.2)

The set $\Pi(U)$ is endowed with a partial order, denoted by $\leq$, with $P \leq P'$ having the meaning

$$\forall C \in P, \exists C' \in P' \text{ such that } C \subseteq C'.$$  \hspace{1em} (3.3)

2Helpers are formally introduced in Section IV. The setting studied in this and the previous section is the one without helpers.
In other words, $\mathcal{P}$ can be obtained from $\mathcal{P}'$ by further partitioning some parts of $\mathcal{P}'$; we then say that $\mathcal{P}$ is finer than $\mathcal{P}'$. We will consider the finest partition in $\Pi'(Z'_U|W)$, the existence of which is guaranteed by the following proposition.

Proposition 7 ([18, Lemma 5.1 and Th. 5.2]): $\Pi^*(Z'_U|W)$ forms a lower semi-lattice with respect to the partial order (3.3). In particular, there is a unique finest partition in $\Pi^*(Z'_U|W)$.

The unique finest partition in $\Pi^*(Z'_U|W)$ is called the fundamental partition, and is denoted as $\mathcal{P}^*(Z'_U|W)$. Again, the unconditional versions of these definitions, namely, $\Pi^*(Z'_U)$ and $\mathcal{P}^*(Z'_U)$, are obtained by dropping the conditioning on $W$ throughout. The fundamental partition has various meaningful interpretations in the problems of vocality [23], [24], successive omniscience [25], data clustering [26], [27] and feature selection [28].

The condition for the optimality of omniscience in [5] and [8] for the PIN model in Definition 5 is expressed in terms of the fundamental partition.

Proposition 8 ([5, Th. 8, Corollary 23]): For the PIN model, we have $R_S = R_{CO}$ iff $\mathcal{P}^*(Z_V) = \{|i| \mid i \in V\}$, namely, the partition into singletons.

The result was based on a lower bound on $R_S$ in [5] that extends the result of [3] to the multiterminal setting using the multi-letter multivariate Wyner common information:

$$C_W := \inf \lim_{n \to \infty} \frac{1}{n} H(L) \text{ such that } \lim_{n \to \infty} \frac{1}{n} I_{\mathcal{P}^*(Z_V)}(Z'_V|L) = 0$$

where the infimum is for a given $Z_V$. Note that $\mathcal{P}^*(Z_V)$ is used instead of $\mathcal{P}^*(Z'_V|L)$. Furthermore, [5] required $L$ to be a function of $Z'_V$, i.e., $H(L|Z'_V) = 0$.

Proposition 9 ([5, Th. 2]): The communication complexity $R_{NR}^S$ with private randomization (2.2) precluded in the problem formulation is lowered bounded as

$$R_{NR}^S \geq C_W - I(Z_V),$$

which holds also with the additional constraint that $H(L|Z'_V) = 0$.

We should mention here that the lower bound to $R_{NR}^S$ derived in [5] involved a quantity called the multiterminal interactive common information, which is always an upper bound to $C_W$. We choose to state the lower bound in (3.5) using $C_W$ since this is enough to derive a sufficient condition for checking whether $R_S = R_{CO}$.

The use of the lower bound in (3.5) is somewhat limited by the difficulty in evaluating the multi-letter expression $C_W$ and the problem formulation that precludes randomization. The derivation of Proposition 9 requires quite a bit of machinery to evaluate $C_W$, and to extend the result to allow randomization. We will improve the bound (in Theorem 13 in Section III-B) with a single-letter expression, for which we need the following definition:

Definition 10: For a finite set $U$ with size $|U| > 1$ and random vector $Z'_U$, the partition Wyner common information of $Z'_U$ with respect to the partition $\mathcal{P} \in \Pi'(U)$ is

$$J_{W,\mathcal{P}}(Z'_U) := \inf \{I(W \wedge Z'_U) \mid I_{\mathcal{P}^*(Z'_U)}(Z'_U|W) = 0\},$$

where the minimum is taken over all possible choices of the random variable $W$ (or $R_{W(Z)}$). $J_{W}(Z'_U \wedge Z'_J)$ denotes the bivariate case $U = \{i, j\}$ where $i \neq j$, and this definition coincides with the usual Wyner common information introduced by [29].

If $\mathcal{P}$ is the partition into singletons, then $J_{W,\mathcal{P}}$ is the extension in [30] of the Wyner common information [29] from the bivariate case $J_{W}(Z'_i \wedge Z'_j)$, to the multivariate case. Following the same argument as in [29], the expression (3.6) is computable with the following bound on support size:

$$|W| \leq |Z'_U|,$$

and inf can be replaced by min, i.e., the infimum can be achieved by a choice of $W$ satisfying (3.7) in addition.

Proof: This follows from the same argument as in [29] and is available in Lemma 5 in Appendix A-A.

Despite the above result, $J_{W,\mathcal{P}}$ is not easy to compute even for the bivariate case [29]. Fortunately, it has a non-trivial entropic bound [18] that is easy to compute:

Proposition 12: $H(Z'_U) \leq J_{W,\mathcal{P}}(Z'_U) \leq J_{D,\mathcal{P}}(Z'_U)$ where

$$J_{D,\mathcal{P}}(Z'_U) := H(Z'_U) - \sum_{C \in \mathcal{P}} H(Z'_C|Z'_{U\setminus C}),$$

which will be called the partition dual total correlation.

Proof: Since $W = Z'_U$ is always a feasible solution to (3.6), $J_{W,\mathcal{P}}(Z'_U) \leq H(Z'_U)$, which gives the first inequality in (3.8). To prove the second inequality, it suffices to show

$$I(W \wedge Z'_U) \geq J_{D,\mathcal{P}}(Z'_U)$$

for all feasible solution $W$. To do so, notice that the constraint (3.6b) means that $Z'_C$ for $C \in \mathcal{P}$ are mutually independent given $W$, and so

$$I(W \wedge Z'_U) = H(Z'_U) - H(Z'_U|W)$$

\begin{align*}
\stackrel{(a)}{=} H(Z'_U) - \sum_{C \in \mathcal{P}} H(Z'_C|W) \\
\stackrel{(b)}{=} H(Z'_U) - \sum_{C \in \mathcal{P}} H(Z'_C|W, Z'_{U\setminus C}) \\
\geq H(Z'_U) - \sum_{C \in \mathcal{P}} H(Z'_C|Z'_{U\setminus C}) \\
= J_{D,\mathcal{P}}(Z'_U),
\end{align*}

where we have applied the independence of $Z'_C$’s in (a) to rewrite $H(Z'_U|W)$ as the sums $\sum_{C \in \mathcal{P}} H(Z'_C|W)$, and in (b) to rewrite $H(Z'_C|W, Z'_{U\setminus C})$.

When $\mathcal{P}$ is the partition into singletons, $J_{D,\mathcal{P}}$ is Han’s dual total correlation [31], which has been shown to be the best entropic lower bound for $J_{W,\mathcal{P}}$ even after incorporating non-Shannon-type inequalities [32].
B. When is $R_S = R_{CO}$?

We begin by giving a single-letter lower bound on $R_S$ that improves upon the result of Proposition 9 by allowing private randomization.

**Theorem 13:** For any source $Z_V$,

$$R_S \geq J_{W,P^*}(Z_V) - I(Z_V)$$

where $P^*$ denotes $P^*(Z_V)$ for convenience,

$$\geq J_{D,P^*}(Z_V) - I(Z_V)$$

and $J_{W,P^*}$ and $J_{D,P^*}$ are the partition Wyner common information (3.6) and the partition dual total correlation (3.9).

**Proof:** See Appendix A-1.

It was shown in [18, Th. 6.3] that $J_{D,P^*}(Z_V)$ is no smaller than $I(Z_V)$ for all $P \in \Pi'(V)$, therefore, the lower bounds above are non-negative. $J_{W,P^*}(Z_V)$ in (3.10a) is the precise single-letterization of $C_W$ in (3.5), so there is no weakening of the lower bound on $R_S$ by allowing randomization. This can be shown by extending the achievability and converse techniques of [29] from two terminals to multiple terminals. In particular, the converse part will be given as part of the proof of the above theorem in the appendix.

**Corollary 14:** $R_S = R_{CO}$ if $J_{W,P^*}(Z_V) = H(Z_V)$.

**Proof:** This follows from Theorem 13 by virtue of (2.9) and Proposition 6, i.e., substituting $J_{W,P^*}(Z_V) = H(Z_V)$ and $I(Z_V) = C_S$ to the right hand side (r.h.s.) of (3.10a) gives $R_{CO}$.

Compared to Proposition 9, (3.10a) is single-letter rather than multi-letter. Furthermore, (3.10b) is a simple linear function of the entropy vector of $Z_V$ given $P^*(Z_V)$, which is easier to evaluate than (3.10a).

From Corollary 14, we obtain the following sufficient condition for the optimality of omniscience under a general source model:

**Theorem 15:** $R_S = R_{CO}$ if

$$H(Z_C|Z_V,C) = 0 \quad \forall C \in P^*(Z_V).$$

where $P^*$ is the fundamental partition in Proposition 7, namely, the finest optimal partition for the MMI (3.1a).

**Proof:** The condition in (3.11) implies that $J_{D,P^*}(Z_V) = H(Z_V)$, and therefore, by (3.8), we also have $J_{W,P^*}(Z_V) = H(Z_V)$. The theorem now follows from Corollary 14.

Condition (3.11) means that, for all $C \in P^*(Z_V)$, no randomness of $Z_C$ is independent of $Z_V|C$. This condition covers all the existing results:

- (3.11) covers the condition for the 2-user case in Proposition 2 because $P^*(Z_{[1,2]}) = \{(1), (2)\}$.
- (3.11) also extends the sufficiency part of the condition in Proposition 8 because (3.11) holds for $P^*(Z_{\{i\}} : i \in V)$ trivially, as every edge variable $X_e (e \in E)$ is a component of $Z_j$ and $Z_k$ for the distinct pair $\{j, k\} = \xi(e)$ of incident nodes.

Despite its generality, (3.11) can be checked easily because $P^*(Z_V)$ can be computed in strongly polynomial-time. The following is an example for which the optimality of omniscience can be easily derived by (3.11) but not by the existing results.

**Example 16:** (3.11) holds for the source in Example 3 as

$$P^*(Z_{[1,2,3]}) = \{(1), (2), (3)\},$$

and $H(Z_1|Z_2, Z_3) = H(Z_2|Z_1) = H(Z_3|Z_1, Z_2) = 0$.

Hence, $R_S = R_{CO}$ by Theorem 15. This example is not covered by Proposition 8 because the private source belongs to the more general finite linear source model [33] rather than the PIN model (Definition 5) or the hypergraphical source model (Definition 4).

C. Stronger Results for Hypergraphical Sources

The necessity of the condition in Proposition 8 can be extended to the more general hypergraphical source model in Definition 4:

**Theorem 17:** For hypergraphical sources with respect to the hypergraph $(V, E, \xi)$, we have $R_S = R_{CO}$ iff

$$\exists e \in E \text{ such that } \xi(e) \subseteq C \text{ for some } C \in P^*(Z_V),$$

which means that there does not exists a hyperedge entirely contained by a part of the fundamental partition, i.e., every hyperedge crosses the fundamental partition.

**Proof:** See Appendix A-2.

$J_{W,P^*}(Z_V)$ can be evaluated for hypergraphical sources because its lower bound by (3.8) is tight:

**Proposition 18:** For hypergraphical sources with respect to the hypergraph $(V, E, \xi)$, we have

$$J_{W,P^*}(Z_V) = H(X_{E^*})$$

where

$E^* := \{e \in E \mid \exists C \in P^*(Z_V), \xi(e) \subseteq C\}$

is the set of hyperedges that cross $P^*(Z_V)$. Furthermore, an optimal solution to (3.6) is $W := (X_e | e \in E^*)$.

**Proof:** See Appendix A-3.

This means that the lower bound (3.10a) can be easily computed for hypergraphical sources. Interestingly, while the lower bound leads to a complete characterization of the optimality of omniscience for the hypergraphical model, it may be loose even for the PIN model when condition (3.12) is not satisfied, as shown by the example below.

**Example 19:** Let $X_a$, $X_b$, and $X_c$ be uniformly random and independent bits. With $V = [3]$, define

$$Z_1 := X_a, \quad Z_2 := (X_a, X_b, X_c), \quad Z_3 := (X_b, X_c),$$

which is a PIN. It can be shown that

$$I(Z_V) = 1 \quad \text{and } P^*(Z_V) = \{(1), (2, 3)\}.$$

The edge $a$ is the only edge that crosses $P^*(Z_V)$. Therefore, $J_{W,P^*}(Z_V) = H(X_a) = 1$, and so (3.10a) gives the trivial lower bound $R_S \geq 1 - 1 = 0$. However, it was proved in [34] that $R_S = 1$ for this example, and so the bound is loose.

---

3Indeed, the bounds in (3.10) hold even if $P^*(Z_V)$ is replaced by any optimal partition $P \in \Pi'(Z_V)$. However, $P^*(Z_V)$ gives the best lower bound because it can be shown that $J_{D,P^*}(Z_V)$ is non-increasing with respect to the partial order $<$ defined in (3.3), by the submodularity of entropy.
D. Limitation of Theorem 15

It turns out that the sufficient condition in Theorem 15 for the optimality of omniscience need not be necessary in general. We demonstrate this using the following example from [35], resolving the conjecture therein.

**Example 20:** Let $X_a, X_b, X_c$ and $X_d$ be uniformly random and independent bits, and define

$$
Z_1 := X_a, \\
Z_2 := X_b, \\
Z_3 := X_c, \\
Z_4 := (X_a, X_b, X_c, X_d), \\
Z_5 := (X_a, X_b, X_d).
$$

It can be shown that

$$
C_S = I(Z_V) = 1 \quad \text{with } P^*(Z_V) = \{[1], [2], [3], [4, 5]\},
$$

$$
R_{CO} = H(Z_V) - C_S = 3
$$

and

$$
J_{W,P^*}(Z_V) = J_{D,P^*}(Z_V) = 3 < H(Z_V) = 4
$$

with $W = (X_{(a,b,c)})$. To achieve the capacity, we can choose for $n = 1$

$$
K := Z_1 = X_a, \\
F_4 := X_c \oplus X_d, \\
F_5 := (X_a \oplus X_b, X_a \oplus X_d),
$$

which also achieves omniscience at the minimum rate.

Note that the sufficient condition (3.11) for the optimality of omniscience does not hold because

$$
H(Z_{[4,5]}|Z_{[1,2,3]}) = H(X_{4}, X_{c} \oplus X_{d}|X_{c}) = 1 > 0.
$$

The following result will show that omniscience is indeed optimal for this example, and so the sufficient condition is not necessary. Furthermore, since the sufficient condition is derived from the lower bound (3.10) on $R_S$, the bound is also loose for this example.

**Proposition 21:** For Example 20, $R_S = R_{CO}$.

**Proof:** See Appendix A-4.

IV. Extensions

In this section, we will briefly discuss extensions of our results to scenarios involving helpers and silent users. We shall begin the discussion by precisely highlighting the role of different types of users in a secret key generation protocol. Next, we shall show that even with helpers and silent users, communication for omniscience still achieves secret key capacity, thereby unifying the results of Csizszár and Narayan [1] and Gohari and Anantharam [2]. We will make a brief mention about how the single-letterization carried out in Theorem 13, and the corresponding sufficient condition for checking the optimality of omniscience in Theorem 15, can be extended to the more general scenario with helpers and silent users. We shall describe in detail the particular scenario involving only trusted helpers and silent users, where new techniques will be used to derive lower bounds on $R_S$ and the corresponding sufficient condition for checking the optimality of omniscience. We will conclude the section by briefly mentioning a class of techniques, which we refer to as the ‘change of scenario’, to obtain lower and upper bounds on $R_S$ for certain instances of the multiterminal source.

A. User Sets and Scenario

In the general secret key agreement problem with helpers and silent users, we still retain the notation $V$ to denote the set of all users. The subset of active users $A \subseteq V$, with $|A| \geq 2$, constitute the set of users who need to agree upon a secret key. The users in $V \setminus A$ are referred to as helpers. The set of helpers are required to communicate in order to help the active users $A$ to generate a secret key, but helpers need not recover the key themselves. Helpers are further subdivided into two categories, trusted helpers $T$ and untrusted helpers $D$. It is required that the key be kept secure from the users in $D$, but not necessarily from the users in $T$. Among the active users $A$, a subset of users $S \subseteq A$ are allowed to be silent during the key generation protocol. We do not consider silent helpers due to the following reasons. It is easy to see that silent trusted helpers can be dropped without having any effect on $C_S$ or $R_S$. On the other hand, it is difficult to handle the case with silent untrusted helpers where even the secret key capacity is not known. Also, by letting $S \subseteq A$, we ensure that there is at least one vocal active user. This is because the secrecy capacity when all active users are silent remains unknown except in the special case with only two trusted users [36] or without helpers. A diagram illustrating the different user sets is provided in Fig. 1.

The vector $(A, S, D, V, Z_V)$ of user sets and private source is called a scenario. Given a scenario, the vocal users discuss in public until the active users can recover a secret key of their choice that is secured against a wiretapper who can listen to the public discussion and wiretap the private source of the untrusted helpers. To carry out the key generation protocol we allow independent private randomness (as in (2.2)) for users in $V \setminus S \setminus S$. It can be shown that allowing private randomness for users in $S \cup D$ does not affect the secret key capacity and the communication complexity, and hence no such randomization is allowed in our formulation. The proof of this fact is a

\[ \text{In the case when all users are active and silent, i.e., } V = A = S, \text{ it is straightforward to show that } C_S = I_{E_{\Delta}(Z_V)} := \max \{H(U) \mid H(U|Z_V) = 0, \forall i \in A\}, \text{ which is the multivariate extension of Gács-Körner common information [37]. We would like to point out here that there is a subtle issue with our preliminary work in [35], in which it was claimed but not proved that the Gács-Körner common information is equal to the secrecy capacity at zero rate of public discussion. We are not able to extend the converse result [37] from no discussion to sub-linear amount (in n) of discussion. Hence, in [35], } C_S \geq I_{E_{\Delta}(Z_V)} \text{ can only be conjectured as a sufficient condition for } R_S \geq 0. \]

\[ \text{For sets } E, F, G, \text{ we will use the notation } E \setminus F \setminus G \text{ to denote the set difference } (E \setminus F) \setminus G. \]
technical exercise, the details of which can be found in [38, Proposition 3.1]. As in Section II, we shall denote by \( U_i \) the private randomization at user \( i \in V \setminus D \setminus S \), and use the notation

\[
\tilde{Z}_i := \begin{cases} (U_i, Z^n_i) & i \in V \setminus D \setminus S \\ Z^n_i & i \in S \cup D \end{cases} \quad \text{(otherwise).} \tag{4.1}
\]

As in the problem without helpers and silent users described in Section II, the vocal users \( V \setminus S \) communicate in a round-robin fashion interactively over a finite number of rounds. We retain the notation \( F \) to denote the communication that has taken place. The notations \( F_i, \hat{F}_i, \text{ and } \hat{F}_D \) in (2.4)-(2.5c) are also retained with the modification that \( F_V \) is now replaced by \( F_{V \setminus S} \). After the communication, the active users in \( A \) are required to agree upon a secret key \( K \), which needs to be secured from the public discussion \( F \), and the observations of the untrusted helpers \( \hat{Z}_D \). In particular, we shall require

\[
\lim_{n \to \infty} \Pr \left( \exists i \in A, K \neq \theta_i(\tilde{Z}_i, F) \right) = 0 \tag{4.2}
\]

and

\[
\lim_{n \to \infty} \left[ \log |K| - H(K| F, \hat{Z}_D) \right] = 0. \tag{4.3}
\]

The secret key capacity \( C_S \) can be defined as in (2.8) as the supremum over all key rates achievable for the given scenario \((A, S, D, V, Z_V)\). Likewise, the communication complexity \( R_S \) can be defined as in (2.12).

**Remark 22:** Our problem formulation covers [1], [2] as special cases:

- Without silent active users, i.e., \( S \subseteq D \), our formulation reduces to that in [1];
- Without trusted helpers, i.e., \( A = V \setminus D \), but at least one vocal active user \( A \setminus S \neq \emptyset \), we obtain the formulation in [2].

### B. Secret Key Capacity and Omniscience

In this section, we shall show that secret key capacity can be achieved using communication for omniscience even in the general setting involving helpers and silent users. We begin by precisely defining an omniscience strategy for secret key agreement.

For \( S \subseteq A \), the omniscience strategy for secret key agreement requires each vocal user \( i \in V \setminus S \) to broadcast in public a function

\[
F_i := f_i(\tilde{Z}_i) = f_i(Z^n_i) \tag{4.4}
\]

of its source such that each active user can first recover the private sources of the untrusted helpers in the sense that

\[
\lim_{n \to \infty} \Pr \left( \exists i \in A, Z^n_D \neq \phi_i(Z^n_i, F_D) \right) = 0 \tag{4.5a}
\]

for some function \( \phi_i \)'s., and then recover the private sources of all other vocal users, i.e.,

\[
\lim_{n \to \infty} \Pr \left( \exists i \in A, Z^n_{V \setminus D \setminus S} \neq \psi_i(\tilde{Z}_i, F_{V \setminus D \setminus S}, Z^n_D) \right) = 0 \tag{4.5b}
\]

for some function \( \psi_i \)'s. Note that the omniscience strategy does not require private randomness. Furthermore, a natural question to ask is whether it is important that \( Z^n_D \) be recovered before the other private sources are. This will be addressed in the subsequent remark and example.

We will further require the omniscience strategy to minimize the total discussion rate, denoted by

\[
R_{CO} := \inf \limsup_{n \to \infty} \frac{1}{n} |F| = \inf \limsup_{n \to \infty} \frac{1}{n} \sum_{i \in V \setminus S} |F_i|, \tag{4.6}
\]

where the infimum being taken over all functions \( f_i, i \in V \setminus S \), that satisfy (4.4)–(4.5). The two recoverability constraints in (4.5) will be called the omniscience constraints, to distinguish them from the recoverability constraint (4.2) for the secret key. For the omniscience strategy to be \( C_S \)-achieving, we will also limit the discussion rates of the untrusted users to satisfy\(^6\)

\[
\left( \lim_{n \to \infty} \frac{1}{n} \log |F_i| \left| i \in D \right. \right) \in \mathcal{R}(Z^n_D) \quad \text{where} \quad \mathcal{R}(Z^n_D) := \{ r_D \in \mathbb{R}^D \mid r(B) \leq H(Z^n_B), \forall B \subseteq D \}. \tag{4.7}
\]

The secret key \( K \) is then chosen as a function of \( Z^n_{V \setminus S} \) at the maximum rate subject to the secrecy constraint (4.3).

**Remark 23:** Instead of (4.5a), [1] requires the entire source of the untrusted user to be revealed in public in the sense that

\[
\lim_{n \to \infty} \Pr \left( Z^n_D \neq \phi(F_D) \right) = 0, \tag{4.9}
\]

i.e., the source of the untrusted users can be recovered not only by the active users but also by anyone who gets to listen to the discussion \( F_D \) by the untrusted users. As will be shown by the following example, \( R_{CO} \) can be strictly larger with this requirement, resulting in a looser upper bound on \( R_S \). The example also shows that (4.5a) and (4.5b) should not be combined into the constraint

\[
\lim_{n \to \infty} \Pr \left( \exists i \in A, Z^n_{V \setminus S} \neq \phi_i(Z^n_i, F) \right) = 0 \tag{4.10}
\]

because even an optimal discussion \( F \) under this constraint can leak too much information to the wiretapper. Hence, omniscience through (4.10) is no longer \( C_S \)-achieving. \( \square \)

**Example 24:** Let \( X_a \) and \( X_b \) be two uniformly random and independent bits, and

\[
Z_1 := X_a \\
Z_2 := (X_a, X_b) \\
Z_3 := X_b \\
Z_4 := (X_a, X_b)
\]

With \( V = [3] \), the source \( Z_V = (Z_1, Z_2, Z_3) \) is a PIN with vertex set \([3]\), edge set \( E = \{a, b\} \) and the edge function

\[
\zeta(e) = \begin{cases} (1, 2) & e = a \\ (2, 3) & e = b. \end{cases}
\]

\(^{6}\)Although the proof of Theorem 25 relies on (4.7), we conjecture that (4.7) is not required for the omniscience strategy to be \( C_S \)-achieving.
With \( V = [4] \) instead, the source \( Z_V \) is not a PIN but a hypergraphically source with the edge function modified to
\[
\zeta(e) = \begin{cases} 
1, 2, 4 & e = a \\
2, 3, 4 & e = b.
\end{cases}
\]

Consider the scenario \((A, S, D, V) = (\{2, 4\}, \emptyset, \{3\}, [4])\). It can be shown that
\[
C_S = 1 \quad \text{and} \quad R_S = R_{CO} = 0,
\]
achieved non-asymptotically with
\[
n = 1, \quad K := X_a \quad \text{and} \quad F \text{ deterministic}.
\]

Hence, omniscience is optimal in this case. Now, if the recoverability condition (4.9) in [1] were imposed instead of (4.5), then \( R_{CO} \geq H(Z_3) = H(X_b) = 1 > 0 = R_S \), and so the omniscience scheme would not be optimal.

Consider the scenario \((A, S, D, V) = (\{1, 2, 4\}, \emptyset, \{3\}, [4])\) instead. It can be shown that
\[
C_S = 1 \quad \text{and} \quad R_S = 0,
\]
achieved non-asymptotically with
\[
n = 1, \quad K := X_a \quad \text{and} \quad F \text{ deterministic}.
\]

However, since the active user 1 does not observe \( X_a \) directly from its private source,
\[
R_{CO} \geq H(Z_V | Z_1) \geq H(X_b) = 1,
\]
which is achieved by choosing \( F := F_3 := X_b \). It follows that \( R_S = 0 < 1 = R_{CO} \), and so omniscience is not optimal. Now, if (4.10) were imposed instead of (4.5), then \( R_{CO} = 1 \) as before but it could be achieved with \( F := F_2 := X_a \oplus X_b \), from which user 1 can recover \( X_b \) as \( F \oplus Z_1 \). However, the wiretapper can also recover \( Z_1 \) as \( F \oplus Z_3 \) by wiretapping the source of the untrusted user 3. Since the entire source, i.e., \( X_a \) and \( X_b \), can be recovered by the wiretapper, any secret key \( K \) satisfying (4.3) must have zero rate. In other words, the current discussion for omniscience, despite being optimal in achieving \( R_{CO} \), leaks too much information to the wiretapper.

Even in the general setting with helpers and silent users the secret key capacity \( C_S \) can still be achieved through a communication for omniscience. This is proved in the following result which also characterizes \( C_S \) and \( R_{CO} \) with helpers and silent users.

**Theorem 25:** With \( S \subseteq A \), the omniscience strategy is \( C_S \)-achieving, with
\[
\begin{align*}
C_S &= H(Z_V \setminus D \setminus S | Z_D) - \rho \\
R_{CO} &= \bar{\rho} + \rho
\end{align*}
\]
where \( \rho \) and \( \bar{\rho} \) are defined as the following linear programs:
\[
\begin{align*}
\rho &:= \min \{ r(V \setminus D, S) | r(V \setminus D \setminus S) \in \mathbb{R}^{\setminus D \setminus S} \}, \\
\bar{\rho} &:= \min \{ r(D) | r(D) \in \mathbb{R}^{\mathbb{R}(Z_D)} \},
\end{align*}
\]
\[
\begin{align*}
r(B) &\geq H(Z_B | Z_V \setminus S, Z_j) \quad \forall j \in A, B \subseteq V \setminus D, S \quad \text{(4.13a)}
\end{align*}
\]
\[
\begin{align*}
r(B) &\geq H(Z_B | Z_D \setminus S, Z_j) \quad \forall j \in A, B \subseteq D. \quad \text{(4.13b)}
\end{align*}
\]
\[
\begin{align*}
r(B) &\geq H(Z_B | Z_V \setminus B, Z_j) \quad \forall j \in A, B \subseteq V \setminus D. \quad \text{(4.14a)}
\end{align*}
\]
\[
\begin{align*}
r(B) &\geq H(Z_B | Z_D \setminus B, Z_j) \quad \forall j \in A, B \subseteq D. \quad \text{(4.14b)}
\end{align*}
\]

**Proof:** See Appendix B-1.

From Theorem 25, we have
\[
R_S \leq R_{CO},
\]
(4.15)

since secret key capacity can always be achieved through omniscience. The single-letter characterizations for \( \rho \) and \( \bar{\rho} \) in (4.13) and (4.14) can be computed in polynomial time, and hence, so can \( C_S \) and \( R_{CO} \). Theorem 25 covers the results of [1] and [2] as the following special cases:

**Corollary 26 (1, Th. 2):** For \( S = \emptyset \),
\[
C_S = H(Z_V \setminus D | Z_D) - \rho \quad \text{where}
\]
\[
\rho = \min \{ r(V \setminus D) | r(B) \geq H(Z_B | Z_V \setminus B), \forall B \in \mathcal{H} \}
\]
and \( \mathcal{H} := \{ B \subseteq V \setminus D | \emptyset \neq B \not\subseteq A \} \). \( \square \)

**Proof:** When \( S = \emptyset \), (4.13b) becomes
\[
r(B) \geq H(Z_B | Z_V \setminus B, Z_j) \quad \forall j \in A, B \subseteq V \setminus D.
\]

This yields the expression in the corollary after removing the redundant constraints where \( B = \emptyset \) or \( B \supseteq j \).

**Corollary 27 (2, Th. 6):** For \( S \subseteq A = V \),
\[
C_S = H(Z_V | S) - \rho \quad \text{where}
\]
\[
\rho = \min \{ r(V \setminus S) | r(B) \geq H(Z_B | Z_V \setminus B), \forall B \in \mathcal{H} \}
\]
and \( \mathcal{H} := \{ B \subseteq V | \emptyset \neq B \not\subseteq A \} \). \( \square \)

**Proof:** With \( S \subseteq A = V \), (4.13b) becomes
\[
r(B) \geq H(Z_B | Z_V \setminus S, Z_j) \quad \forall j \in A, B \subseteq V \setminus S.
\]

The constraints with \( B \ni j \) are again redundant and so we can impose \( j \notin B \). With \( B' = B \cup S \setminus \{j\} \), the constraints can be rewritten as
\[
r(B' \setminus S) \geq H(Z_B' | Z_V \setminus B').
\]

The constraints can only be weaker if some element in \( S \) is removed from \( B' \), as the r.h.s. cannot increase but the l.h.s. remains unchanged. This yields the expression in the corollary.

As illustrated by Example 24, \( \bar{\rho} \) can be strictly smaller than \( H(Z_D) \), i.e., the omniscience strategy is an improved version of that [1] when \( S = \emptyset \neq D \). Consequently, the \( R_{CO} \) upper bound (4.15) is also improved.

C. Single-Letter Lower Bounds and Sufficient Conditions

As in the case with no helpers and silent users, a single-letter lower bound to bound \( R_S \) in the general setting with helpers and silent users can be derived by suitably defining a conditional version of Wyner common information. Using that lower bound one can also come up with a sufficient condition to check for the optimality of omniscience. The entire exercise is similar to the one carried out for the case with no helpers and silent users in Section III with some added technicalities.

Hence, we have decided to relegate it to a technical report [38, Secs. VLA–VLC]. However, we are able to derive a different set of lower bounds on \( R_S \) for the specific scenario

\[ \text{7This can be argued as in } [13] \text{ by noting that the separation oracle corresponds to performing a polynomial number of submodular function minimizations, which can be done in polynomial time.} \]
where $S \subseteq A = V$. These bounds turn out to be better than the lower bounds derived using the ‘conditional’ Wyner common information, and this section is devoted to studying them.

Throughout this section, we only consider the scenario $S \subseteq A = V$, i.e., all the users are active but some of them may be forced to be silent. We begin by providing an alternate characterization of the secrecy capacity in [2, Th. 6].

**Proposition 28:**

\[
C_S = \begin{cases} 
\min_{i \in S} I(Z_{V \setminus S} \wedge Z_i) & \text{if } |V \setminus S| = 1 \\
\min(a, I(Z_{V \setminus S})) & \text{if } |V \setminus S| > 1,
\end{cases}
\]  

(4.16a)

where $a := \min_{i \in S} I(Z_{V \setminus S} \wedge Z_i)$.

**Proof:** See Appendix B-2.

We now turn our attention to lower bounding $R_S$ for the case with $S \subseteq A = V$. For this, we introduce some convenient notation, starting with the definition

\[
S^* := \{ i \in S \mid I(Z_{V \setminus S} \wedge Z_i) = a \},
\]  

(4.17)

where $a$ is as defined in Proposition 28. We extend the notation introduced in Theorem 13: for any $U \subseteq V$, the $P^*$ in the subscripts of $J_{W, P^*} (Z_U)$, $J_{D, P^*} (Z_U)$ and $I_{P^*} (Z_U)$ denotes the fundamental partition $P^*(Z_U)$.

Applying the lower bound in Theorem 13 with an appropriate choice of $U$ and $P \in \Pi (U)$ yields the following result.

**Theorem 29:**

\[
R_S \geq \begin{cases} 
J_{W, P^*} (Z_{V \setminus S}) - I(Z_{V \setminus S}) & \text{if } I(Z_{V \setminus S}) < a \text{ and } |V \setminus S| > 1, \\
\max_{i \in S^*} J_{W, P^*} (Z_{V \setminus S} \wedge Z_i) - a, & \text{if } |V \setminus S| = 1,
\end{cases}
\]  

(4.18a)

\[
\max_{i \in S^*} J_{W, P^*} (Z_{V \setminus S} \wedge Z_i) - a, & \text{if } |V \setminus S| = 1,
\end{cases}
\]  

(4.18b)

where $S^*$ is as defined in (4.17).

**Proof:** See Appendix B-2.

The lower bounds in Theorem 29 can be weakened by replacing $J_{W, P}$ with the more easily computable $J_{D, P}$. Using arguments similar to those in Section III, we arrive at the following sufficient condition for $R_S = R_{CO}$ to hold.

**Theorem 30:** $R_S = R_{CO}$ in either of the following scenarios:

(i) $H(Z_C | Z_{V \setminus C}) = 0$, $\forall C \in P^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < a$,

(ii) $\exists i \in S^*$ such that $H(Z_{V \setminus S} | Z_i) = 0$, when $|V \setminus S| = 1$, or when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > a$,

(iii) $\exists i \in S^*$ such that $H(Z_{C} | Z_{V \setminus S} \cup \{i\}, Z_i) = 0$, $\forall C \in P^*(Z_{V \setminus S} \cup \{i\})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = a$.

where $S^*$ is as defined in (4.17).

**Proof:** See Appendix B-2.

The lower bounds in Theorem 29 can be strengthened for the specific case of the hypergraphical source. This in turn strengthens the sufficient conditions for $R_S = R_{CO}$ given in Theorem 30. We will show that the strengthened conditions are both necessary and sufficient for $R_S = R_{CO}$ to be valid.

The idea is based on the following observation.

**Proposition 31:** For any hypergraphical source, $(V, E, \zeta)$, $C_S$, $R_S$ and $R_{CO}$ remain unchanged by removing any hyper-edge $e' \in E$ such that $\zeta(e') \subseteq S$.

**Proof:** See Appendix B-2.

Thanks to this fact we will assume that the hypergraphical sources considered later in this section satisfy

\[
\forall e \in E, \quad \zeta(e) \subseteq S.
\]  

(4.19)

Using (4.19), the lower bound in Theorem 29 can be strengthened to the following for the hypergraphical source.

**Theorem 32:** For any hypergraphical source $(V, E, \zeta)$ with $S \subseteq A = V$, we have

\[
\begin{align*}
J_{W, P^*} (Z_{V \setminus S}) - I(Z_{V \setminus S}) & \quad \text{if } I(Z_{V \setminus S}) < a \text{ and } |V \setminus S| > 1, \\
J_{W, P^*} (Z_{V \setminus S} \cup \{i\}) (Z_{V \setminus S} | S^*) & - a, & \text{if } |V \setminus S| = 1, \\
J_{W, P^*} (Z_{V \setminus S} \cup \{i\}) (Z_{V \setminus S} | S^*) & - a, & \text{if } |V \setminus S| = 1 \text{ and } |V \setminus S| > 1, \\
I(Z_{V \setminus S}) & = 1, & \text{if } |V \setminus S| = 1 \text{ and } |V \setminus S| > 1,
\end{align*}
\]  

(4.20a)

where $S^*$ is as defined in (4.17).

**Proof:** See Appendix B-2.

The results of Theorem 32 can be used to obtain sufficient conditions for $R_S = R_{CO}$ to hold, by following the same steps as in the proof of Theorem 30. Fortunately, it turns out that those conditions are also necessary, a fact that can be proved using the idea of incremental secret key agreement highlighted in [11] and [12].

**Theorem 33:** For any hypergraphical source $(V, E, \zeta)$ with $S \subseteq A = V$, we have $R_{CO} = R_S$ iff

(i) $H(Z_C | Z_{V \setminus C}) = 0$, $\forall C \in P^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < a$,

(ii) $H(Z_{V \setminus S} | Z_{S^*}) = 0$, when $|V \setminus S| = 1$ or, if $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > a$,

(iii) $H(Z_C | Z_{(V \setminus S) | S^*}) = 0$, $\forall C \in P^*(Z_{V \setminus S})$, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = a$.

**Proof:** See Appendix B-2.

We remark here that the lower bounds and sufficient conditions derived so far (Theorems 15–17 and Theorems 29–33) can all be extended to the case with untrusted helpers by further conditioning on $Z_U$ in the entropies. For hypergraphical sources, this is equivalent to removing the hyperedges incident on $D$.

**D. Change of Scenario**

Change of scenario refers to a broad class of techniques which can be used to derive lower and upper bounds on $R_S$ for certain instances of the multiterminal source. Some of these bounds can also be used to derive necessary or sufficient conditions for optimality of omniscience. In fact, the decremental secret key agreement described in Proposition 36 (needed to prove Theorem 17) is a change of scenario technique. Broadly speaking, such techniques look at a pair of scenarios where one scenario is obtainable from the other by modifying the different user sets. For example, one can make a group of silent
users into vocal active users, thereby changing the scenario. If such a change does not affect \( C_S \), and any secret key capacity achieving scheme for one scenario can be used to obtain a maximum rate secret key for the other scenario as well, then \( R_S \) of the first scenario can be used as upper bound to \( R_S \) of the second scenario. Further, if appropriate bounds are known for \( R_S \) for one of these scenarios, they can be translated to bounds on \( R_S \) for the other scenario. A multitude of these change of scenario techniques can be devised, and we shall illustrate one such technique here. We have compiled a list of such techniques in [38, Secs. V.B and VII.B].

To begin with, we shall be denoting the pair of scenarios by \((A, S, D, V, Z_V)\) and \((A', S', D', V', Z_{V'})\). Also, the secret key capacity, minimum rate of communication for omniscience, and the communication of the two scenarios are denoted respectively by \((C_S, R_{CO}, R_S)\) and \((C_S', R_{CO}', R_S')\). We now describe a change of scenario technique which can be used to obtain an upper bound to \( R_S \). Using the upper bound we shall also derive a necessary condition for the optimality of omniscience. Consider the situation when a proper subset of vocal active users are converted to silent active users, while all trusted helpers are removed. Therefore, we have \( A' = A, T' = V' \backslash A' \setminus D' = \emptyset, D' = D, \) and \( S' \supseteq S \). The change is depicted in Fig. 2. In addition suppose that this change preserves secret key capacity, i.e., \( C_S = C_S' \).

We claim that

\[
R_S \leq R_S' \leq R_{CO}' \leq R_{CO}.
\]

Further, it follows that \( R_S = R_{CO} \) only if

\[
H(Z_{V \backslash S'}) = H(Z_{V \backslash S}).
\]

It is simple to argue that any \( R_S \leq R_S' \) as any capacity achieving scheme for the modified scenario is a capacity achieving scheme for the original scenario. To complete the proof of (4.21), we need to show \( R_{CO}' \leq R_{CO} \), since \( R_S' \leq R_{CO} \) using (4.15). Suppose \( (\rho, \bar{\rho}) \) becomes \( (\rho', \bar{\rho}') \) in the new scenario. Note that \( \bar{\rho} = \bar{\rho}' \) if the sets \((A, D)\) remain unchanged. We also have (4.11), that

\[
\rho' = \rho - \frac{H(Z_{V \backslash D}) - H(Z_{(V \backslash D) \setminus S} | Z_D)}{\bar{\rho}}.
\]

by noting that \( A \setminus S' = (V' \setminus D) \setminus S' \). Here,

\[
\beta = H(Z_{V \setminus S}) - H(Z_{V' \setminus S'}) \\
= H(Z_{(S' \setminus S) \cup (V' \setminus V)}) Z_{V \setminus S} \geq 0.
\]

Hence, by (4.15), \( R_{CO}' = \rho' + \rho' = \bar{\rho} + \rho - \beta \leq \bar{\rho} + \rho = R_{CO} \), which completes the proof of (4.21).

We present below a specific example where this particular change of scenario technique can be used to prove that \( R_S < R_{CO} \).

Example 34: Consider Example 1 with \( A = V = \{1, 2\}, D = S = \emptyset, Z_1 = (X_0, X_1) \) and \( Z_2 = (X_1, J) \). If we choose \( S' = \{1\} \) and everything else the same, then condition (4.22) fails because \( H(Z_2) = 2 < 3 = H(Z_{\{1,2\}}) \). Hence, by (4.22), we have \( R_S < R_{CO} \) as expected.

\[\Box\]

V. Concluding Remarks

In this paper we have identified sufficient conditions for which \( R_S = R_{CO} \) holds in the multiterminal source model, possibly with helpers and silent users. The sufficient condition to check whether \( R_S = R_{CO} \) also turns out to be necessary for the special case of the hypergraphical source. However, we show using an example that the necessity of the conditions does not extend beyond the hypergraphical sources. The derivation of these conditions rely on the single-letterization of a lower bound on \( R_S \) derived in [5]. Our results also allow private randomization at each user. We have described in detail the process of single-letterization for the case without helpers and silent users, and made a brief mention of the extension to the setting with helpers and silent users. A more detailed treatment has been compiled in the technical report [38]. In order to study the case with helpers and silent users, we derived an expression for the minimum rate of communication for omniscience in that setting, thereby unifying the results of [1] and [2]. We also developed a class of techniques called the change of scenario to obtain lower and upper bounds on \( R_S \), and to possibly translate them to conditions for checking whether \( R_S = R_{CO} \).

We would like to remark that obtaining an exact condition to identify sources satisfying \( R_S = R_{CO} \) is still open for the general multiterminal source. We believe that an exact characterization is possible by suitably strengthening the lower and upper bounds on \( R_S \). The bigger problem of characterizing \( R_S \) itself remains open. It is also not known whether \( R_S \) remains unchanged if private randomization is allowed at each user. There are recent works [34], [39] exploring other techniques and problem formulations. As pointed out in [34], the lower bound in (3.10a) on \( R_S \) can be loose even for a simple PIN involving three users. Instead of using the Wyner common information, the techniques in [34] can sometimes give better bounds. For the PIN model, in particular, we have a complete characterization of \( R_S \) as well as the entire trade-off between the achievable secret key rate and total discussion rate. However, the bound can be worse for hypergraphical sources, and it remains unclear whether these different techniques can be unified seamlessly with the techniques in the current work.

APPENDIX A

PROOFS FOR SECTION III

1. Proof of Theorem 13

It is enough to prove (3.10a), since (3.10b) then follows from (3.8). Let \( U_V \) be the optimal sequence of randomization...
that achieves $R_S$, and let $R_{S}^{NR}(\tilde{Z}_V)$ be the communication complexity when the source $Z_V$ is changed to $\tilde{Z}_V$ instead (see (2.3) for the definition of $\tilde{Z}_V$). Then,

$$R_S(\tilde{Z}_V) \geq \frac{1}{n} R_{S}^{NR}(\tilde{Z}_V) \geq \frac{1}{n} [C_W(\tilde{Z}_V) - I(\tilde{Z}_V)]$$

(c) $\frac{1}{n} [nJ_{W,P^\ast}(Z_V) - I(\tilde{Z}_V)]$

(d) $J_{W,P^\ast}(Z_V) - I(\tilde{Z}_V)$

To explain (a), note that the secrecy capacity of the source $\tilde{Z}_V$ is $nC_S$, since randomization does not change the secrecy capacity [1]. Any optimal scheme that achieves $R_S$ for the original source can therefore be translated directly to a scheme that achieves $nR_S$ for the new source $\tilde{Z}_V$ without randomization.

(b) is by Proposition 9 with $Z_V$ replaced by $\tilde{Z}_V$, and $C_W(\tilde{Z}_V)$ denoting the corresponding multi-letter multivariate Wyner common information (3.4).

(c) follows from

$$C_W(\tilde{Z}_V) \geq nJ_{W,P^\ast}(Z_V), \quad (A.1)$$

which will be argued in more detail later using the converse technique in [29] for the Wyner common information. Although not needed for the current result, the reverse inequality of (A.1) can also be argued by extending the achievability result in [29] from two terminals to multiple terminals. Hence, the single-letterization does not weaken the bound (3.5) on $R_{S}^{NR}$. The converse is also stronger as it allows for private randomization.

To explain (d), note that for all $B \subseteq V$,

$$H(\tilde{Z}_B) = H(Z_V^n, U_B) = nH(Z_V) + H(U_B),$$

which gives

$$I_{\mathcal{P}}(\tilde{Z}_V) = nI_{\mathcal{P}}(Z_V) + I_{\mathcal{P}}(U_B)$$

for all $\mathcal{P} \in \Pi'(V)$. Since $I_{\mathcal{P}}(U_B) = 0$ by the fact that the $U_i$’s are mutually independent (2.2), the above equation implies $I(\tilde{Z}_V) = nI(Z_V)$ as desired.

To explain (A.1), consider the optimal sequence in $n'$ to $C_W(V)$. By standard arguments,

$$H(L) \geq I(\tilde{Z}_V^n \land L) \geq I(\tilde{Z}_V^n \land L)$$

$$= H(Z_V^n) - H(Z_V^n | L)$$

$$= \sum_{t=1}^{n'} H(Z_{Vt}) - \sum_{t=1}^{n'} H(Z_{Vt} | Z_{V}^{t-1}, L)$$

where the second inequality follows from the usual data processing inequality since $Z_V$ is determined by $\tilde{Z}_V$, and so, we have the Markov chain $L - \tilde{Z}_V^n - Z_{V}^{n'}$. Let $J$ be the usual time-sharing random variable uniformly distributed over $[n'n]$ and independent of everything else, namely $(\tilde{Z}_V^n, L)$, and define

$$W_J := (J, Z_{V}^{t-1}, L).$$

Then, the above inequality gives

$$\frac{1}{n} H(L) \geq nI(Z_{V}^{n'} \land W_J). \quad (A.2)$$

On the other hand, we can also bound $I_{\mathcal{P}}$ in the constraint (3.4b) of $C_W$ as follows:

$$I_{\mathcal{P}}(\tilde{Z}_V^n | L) \geq I_{\mathcal{P}}(Z_V^n | W) - H(Z_V^n | W)$$

$$= \frac{1}{|\mathcal{P}|} \left[ \sum_{C \in \mathcal{P}} H(Z_V^n | W_C) - H(Z_V^n | W) \right]$$

where, as in the statement of the theorem, $\mathcal{P}^\ast$ denotes $\mathcal{P}^\ast(\tilde{Z}_V)$ for convenience. In the above inequality, we have applied $P^\ast(\tilde{Z}_V) = P^\ast(Z_V)$ and the data processing inequality [18, eq. (5.20b)] since $Z_{V}^{n}$ is determined by $\tilde{Z}_I$. Expanding $\circledast$ and $\circledast$ by the chain rule,

$$\begin{align*}
\circledast &= \sum_{t=1}^{n'} H(Z_{Ct} | L, Z_{V}^{t-1}) \\
&\geq \sum_{t=1}^{n'} H(Z_{Ct} | L) - H(Z_{Ct} | W) \\
&= nI_{\mathcal{P}}(Z_{V}^{n} | W_J).
\end{align*}$$

Altogether, we have

$$\frac{1}{n} I_{\mathcal{P}}(\tilde{Z}_V^n | L) \geq \frac{n}{|\mathcal{P}|} \left[ \sum_{c \in \mathcal{P}} H(Z_{Ct} | L) - H(Z_{Ct} | W) \right]$$

$$= nI_{\mathcal{P}}(Z_{V}^{n} | W_J). \quad (A.3)$$

Now, for $\delta \geq 0$, define

$$\Gamma(\delta) := \sup_{P_{WZ_{V}} \in \Pi(\tilde{Z}_V) | H(Z_{V}^{n} | W) \leq \delta} H(Z_{V}^{n} | W), \quad (A.4)$$

where the supremum is over all possible choices of the conditional distribution $P_{WZ_{V}}$. The expression depends implicitly on the distribution $P_{Z_{V}}$. It follows that

$$\Gamma \left( \frac{1}{n} \right) \sup_{n' \to \infty} n I_{\mathcal{P}}(Z_{V}^{n'} | L) \geq H(Z_{V}^{n'} | W_J)$$

since $Z_{V}^{n'}$ has the same distribution as $Z_{V}$ and so the conditional distribution $P_{WJZ_{V}}$ is a feasible solution to (A.4) with $\delta$ chosen appropriately from the bound (A.3) on $I_{\mathcal{P}}(Z_{V}^{n'} | W_J)$. Together with (A.2), we have

$$C_W(\tilde{Z}_V) \geq \lim_{n' \to \infty} n \left[ H(Z_{V}^{n'} | W) - \Gamma \left( \frac{1}{n} \right) I_{\mathcal{P}}(Z_{V}^{n'} | L) \right]$$

$$= n \left[ H(Z_{V}) - \lim_{\delta \to 0} \Gamma(\delta) \right]$$

where the last equality is because $H(Z_{V}^{n'}) = H(Z_{V})$ and $\frac{1}{n} I_{\mathcal{P}}(Z_{V}^{n'} | L)$ goes to 0 as $n'$ goes to $\infty$ by the constraint (3.4b) for $C_W(\tilde{Z}_V)$. It can be shown that $\Gamma(\delta)$ is continuous in $\delta$ using the same argument as in [29]. For completeness,
this is proved for the more general case in Lemma 35 which follows. Hence,
\[
C_W(\tilde{Z}_V) \geq n \left[ H(Z_V) - \Gamma(0) \right] = n J_{W,p}(Z_V)
\]
by the definition (3.6) of \( J_{W,p} \).

**Lemma 35:** It is admissible to impose in (A.4) that
\[
|W| \leq \begin{cases} 
|Z_U| + 1 & \delta > 0 \\
|Z_U| & \delta = 0,
\end{cases}
\]
and so sup in (A.4) can be replaced by max and \( \Gamma(\delta) \) is continuous in \( \delta \).\(^8\)

**Proof:** Pick any \( Z_U' \in Z_U \), and define \( S \) as the set of all possible vectors of values for
\[
(H(Z_U | W = w), I_P(Z_U | W = w)), \quad P_{Z_U | W = w}(Z_U) | z_U \in Z_U \setminus |Z_U'| \).
\]
There is a one-to-one mapping between the choice of \( P_{Z_U | W = w} \) and the choice of \( v(w) \in S \), noting that
\[
P_{Z_U | W = w}(Z_U') = 1 - \sum_{z \in Z_U \setminus |Z_U'|} P_{Z_U | W = w}(Z_U).
\]
Thus, a feasible solution to (A.4) corresponds to a choice of a set \( W \), a distribution \( P_W \) over \( W \), and a vector \( v(w) \) for every \( w \in W \), such that
\[
\sum P_W(w)v(w) = (H(Z_U | W), I_P(Z_U | W), P_{Z_U | W}(Z_U) | z_U \in Z_U \setminus |Z_U'|).
\]
By the Fenchel-Eggleston-Carathéodory theorem [40], it is admissible to choose \( |W| \) equal to the length of \( v(w) \) plus 1, i.e., \( |Z_U| + 1 \) as desired in (A.5) for \( \delta \geq 0 \). If \( \delta = 0 \), i.e., one requires \( I_P(Z_U | W) = 0 \), then \( I_P(Z_U | W = w) = 0 \) for all \( w \in W \) since \( I_P \) is non-negative by (3.1b). In other words, the constraint is on individual choice of \( P_{Z_U | W = w} \), and so we can redefine \( S \) without having \( I_P(Z_U | W = w) \) as a component of \( v(w) \), i.e., which gives the smaller bound in (A.5).

Suppose there is a sequence in \( k \) of choices of \((P_{W_k}, P_{Z_U | W_k})\) that attains \( \Gamma(\delta) \) in the limit as \( k \to \infty \) while satisfying the constraint in (A.4), i.e.,
\[
I_P(Z_U | W_k) \leq \delta.
\]
By imposing (A.5) such that \( W \) is finite with size independent of \( k \), the feasible choices of \((P_{W_k}, P_{Z_U | W_k})\) form a compact set. Hence, there exists a subsequence \( \{k_j\}_{j=1}^\infty \) such that
\[
P_W = \lim_{j \to \infty} P_{W_{k_j}} \text{ and } P_{Z_U | W} = \lim_{j \to \infty} P_{Z_U | W_{k_j}}.
\]
By the continuity of entropy [4], we also have
\[
I_P(Z_U | W) = \lim_{j \to \infty} I_P(Z_U | W_{k_j}), \quad (A.9a) \quad \text{and} \quad H(Z_U | W) = \lim_{j \to \infty} H(Z_U | W_{k_j}). \quad (A.9b)
\]
Note that the r.h.s. of (A.9a) is upper bounded by \( \delta \) since each term in the limit is. Furthermore, the r.h.s. of (A.9b) attains \( \Gamma(\delta) \) by assumption. Hence, the supremum in (A.4) is achieved by the above choice of \( W \), i.e., the sup in (A.4) can be replaced by max.

Consider proving the continuity of \( \Gamma(\delta) \). Consider any sequence \( \{\delta_k\}_{k=1}^\infty \) such that \( \delta_k > \delta \) and \( \delta_k \downarrow \delta \) as \( k \to \infty \).

Possible vectors of values for \( \delta \).

\[
\Gamma(\delta) \leq \lim_{k \to \infty} \Gamma(\delta_k). \quad (A.10)
\]
Let \((P_{W_k}, P_{Z_U | W_k})\) be the optimal solution for \( \Gamma(\delta_k) \). Then, as argued previously, \((P_{W}, P_{Z_U | W})\) exists satisfying (A.8) and (A.9) for some subsequence \( \{k_j\}_{j=1}^\infty \). Furthermore, the r.h.s. of (A.9a) is equal to \( \lim_{k \to \infty} \delta_k = \delta \), and so \( W \) is a feasible solution to (A.4). The l.h.s. of (A.9b) is therefore upper bounded by \( \Gamma(\delta) \) and so
\[
\Gamma(\delta) \geq \lim_{k \to \infty} \Gamma(\delta_k),
\]
which is satisfied with equality by (A.10), implying that \( \Gamma(\delta) \) is continuous in \( \delta \). \( \square \)

2. **Proof of Theorem 17**

To prove Theorem 17, we use the idea of decremental secret key agreement [11, 12].

**Proposition 36** ([11, Th. 4.2], [12, Th. 5.8]): If \( Z_V \) can be rewritten for some non-empty set \( T \subseteq C \in P^*(Z_V) \) as
\[
Z_i = \left\{ \tilde{Z}_i, X \right\} \forall i \in T, \quad \tilde{Z}_i = Z_i \forall i \in V \setminus T,
\]
where \( H(X) = H(X_\tilde{V}) > 0 \), then, we have
\[
H(Z_V) < H(Z_V) \quad \text{and} \quad I(Z_V) = I(Z_V)
\]
for some function \( Z'_i = \vartheta_i(Z_i) \) for \( i \in V \).

Let us explain the result stated in Proposition 36 using the following example.

**Example 37:** Let \( |V| = 4 \) and consider the source \( Z_V \) defined as follows.
\[
\begin{align*}
Z_1 & := (X_a, X_b, X_c) \\
Z_2 & := (X_a, X_b, X_d) \\
Z_3 & := (X_c, X_t) \\
Z_4 & := (X_d, X_e)
\end{align*}
\]
Here \( X_a, X_b, X_c, X_d, X_e \) are i.i.d. uniform bits. Note that the source \( Z_V \) satisfies the hypothesis of Proposition 36. In particular, we can choose \( T = \{1, 2\}, X = X_b, \tilde{Z}_1 = (X_a, X_c), \tilde{Z}_2 = (X_a, X_d), \text{ and } Z_i = Z_i \text{ for } i = 3, 4. \) It is not difficult to show that \( I(Z_V) = 1.5 \). Now consider the random variable \( X_b' \) obtained by processing \( X_b \) independent of all the other random variables, such that \( H(X_b') = 0.5 \). Then we can define the processed source \( Z_V' \) as follows. We let \( Z_1' = (X_a, X_b', X_c), Z_2' = (X_a, X_b', X_d), \text{ and } Z_i' = Z_i \text{ for } i = 3, 4. \) Therefore, we have \( 4.5 = H(Z_V') < H(Z_V) = 5 \). Also, it is easy to see that the processed source \( Z_V' \) satisfies \( I(Z_V') = 1.5 \). \( \square \)

To prove Theorem 17 we use the following argument. Roughly speaking, when (3.11) fails for hypergraphical sources, using Proposition 36 we can identify and reduce
excess randomness in the source without changing $C_S$, and so omniscience is not optimal in achieving $R_S$.

The "if" case of Theorem 17 follows from Theorem 15 directly. To prove the "only if" part, suppose to the contrary that

$$H(Z_C | Z_{V \setminus C}) > 0 \text{ for some } C \in \mathcal{P}^*(Z_V).$$

For hypergraphical model, this means that

$$H(X_{e'} | Z_{V \setminus C}) > 0 \text{ for some } e' \in E,$$

i.e., $\xi(e') \subseteq C$. Thus, (A.11) holds with $X := X_{e'}, T := \xi(e') \subseteq C$ and

$$\tilde{Z}_i := (X_{e'} | e \in E \setminus e', i \in \xi(e)).$$

By Proposition 36, we have (A.12). With $R'_S$ and $R'_{CO}$ denoting the communication complexity and the smallest rate of CO for the source $Z'_V$, we have

$$R_S \leq R'_S \leq R'_{CO} = H(Z'_V) - I(Z'_V)$$

$$< H(Z_V) - I(Z_V) = R_{CO}(Z_V),$$

where (a) is due to the fact that processing $Z_i$'s individually cannot reduce the communication complexity $R_S$; and (b) is by (A.12). This completes the proof of Theorem 17.

3. Proof of Proposition 18

First, observe that with $W = (X_{e'} | e \in E^*)$, using the assumption that the random variables $X_{e'}$'s are mutually independent, we have

$$\sum_{C \in \mathcal{P}^*} H(Z_C | W) = \sum_{C \in \mathcal{P}^*} H(X_{e' \in E' \setminus \xi(e) \subseteq C})$$

$$= H(X_{e'} | H(E') = H(Z_V | W))$$

Hence, $I_{W, \mathcal{P}^*}(Z_V | W) = 0$, and so $W$ is a feasible solution to $J_{W, \mathcal{P}^*}(Z_V)$. Thus, $J_{W, \mathcal{P}^*}(Z_V) \leq H(X_{e'}^*)$. By (3.8), On the other hand, we also have, by (3.8),

$$J_{W, \mathcal{P}^*}(Z_V) \geq H(Z_V) - \sum_{C \in \mathcal{P}^*} H(Z_C | Z_{V \setminus C})$$

$$= H(X_{e'}) - \sum_{C \in \mathcal{P}^*} H(X_{e' \in E' \setminus \xi(e) \subseteq C})$$

$$= H(X_{e'}) - H(X_{e' \in E'})$$

$$= H(X_{e'}).$$

Thus, $J_{W, \mathcal{P}^*}(Z_V) = H(X_{e'})$ with $W = (X_{e'} | e \in E^*)$ being an optimal solution.

4. Proof of Proposition 21

To prove the desired result, we will make use of the following independence relation satisfied by the private source:

$$0 = I(\tilde{Z}_1 \wedge \tilde{Z}_2) = I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,4]}) = I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,5]}).$$

(A.13)

The desired conclusion will be proved by showing the stronger result that

$$\limsup_{n \to \infty} \frac{1}{n} \left[ H(F_{[4,5]}) - 3H(K) \right] \geq 0$$

(A.14)

which implies $R_S \geq 3C_S = 3 = R_{CO}$ as desired.

To prove the above, define

$$a_t := I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_{[4]}^t) - I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_{[4]}^{-1})$$

(A.15a)

$$b_t := I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,4]} | F_{[4]}^t) - I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,4]} | F_{[4]}^{-1})$$

(A.15b)

$$c_t := I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,5]} | F_{[4]}^t) - I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,5]} | F_{[4]}^{-1})$$

(A.15c)

By definition of (A.15), we have

$$\sum_{t=1}^{r} (a_t + b_t + c_t)$$

$$= I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F) + I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,4]} | F) + I(\tilde{Z}_3 \wedge \tilde{Z}_{[1,2,5]} | F)$$

$$\geq 3H(K) - 3n\delta_n$$

for some $\delta_n \to 0$ as $n \to \infty$. Here, the inequality follows from the recoverability (2.6) and secrecy (2.7) requirement, for instance, $I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F) \geq I(\tilde{Z}_1 | K \wedge \tilde{Z}_2 | K | F) - \frac{ak}{2} \geq H(K) - n\delta_k$. Then, it suffices to show that

$$H(F_{[4,5]}) \geq \sum_{t=1}^{r} (a_t + b_t + c_t).$$

(A.16)

To achieve this, we will bound $a_t$, $b_t$ and $c_t$ one by one. We first bound $a_t$ as follows:

$$a_t \equiv I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1}, \tilde{Z}_1) - I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1})$$

(A.15a)

$$\equiv I(F_{V_1} \wedge \tilde{Z}_{[1,2]} | F_{[4]}^{-1}) - I(F_{V_1} \wedge \tilde{Z}_{[1,2]} | F_{[4]}^{-1}) - I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1})$$

(A.15a)

$$\equiv I(F_{[1,2]} | F_{[4]}^{-1})$$

(A.15a)

$$\equiv I(F_{[1,2]} | F_{[4]}^{-1}) + I(F_{[1,2]} | F_{[4]}^{-1}, \tilde{Z}_1)$$

(A.15a)

$$\equiv I(F_{[1,2]} | F_{[4]}^{-1}) - I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1})$$

(A.15a)

$$\leq I(F_{[3,4,5]} | \tilde{Z}_{[1,2]} | F_{[4]}^{-1}, F_{[1,2]} | F_{[4]}^{-1})$$

(A.15a)

where (a) is due to the fact that

$$I(\tilde{Z}_1, F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1})$$

$$= I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_{[4]}^{-1}) + I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1}, \tilde{Z}_1)$$

$$= I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1}) + I(\tilde{Z}_1 \wedge \tilde{Z}_2 | F_{[4]}^{-1}),$$

(b) and (c) are due to the chain rule expansion, (d) is due to the fact that

$$I(F_{[1,2]} | F_{[4]}^{-1}) = H(F_{[1,2]} | F_{[4]}^{-1})$$

by (2.4), (e) is due to the fact that

$$I(F_{V_1} \wedge \tilde{Z}_2 | F_{[4]}^{-1}, F_{[1,2]} | F_{[4]}^{-1})$$

$$\geq I(F_{1} | F_{[4]}^{-1}) + I(F_{1} | F_{[4]}^{-1}, \tilde{Z}_2 | F_{[4]}^{-1})$$

$$\geq I(F_{1} | F_{[4]}^{-1}) + I(F_{2} | F_{[4]}^{-1}, F_{1} | F_{[4]}^{-1})$$

$$= H(F_{1} | F_{[4]}^{-1}) + H(F_{1} | F_{[4]}^{-1}, F_{1} | F_{[4]}^{-1})$$

$$= H(F_{[1,2]} | F_{[4]}^{-1})$$

(A.14)
We then bound \( b_1 \) as follows:

\[
\begin{align*}
\quad b_1 &\overset{(a)}{=} I(F_{V't} \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}, \tilde{Z}_3) - I(F_{V'} \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}) \\
&\overset{(b)}{=} I(F_{V'} \wedge \tilde{Z}_{1,2,3,4}|F_{V'}^{-1}) - I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
&\quad - I(F_{V'} \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}) \\
&\overset{(c)}{\leq} H(F_{V'}|F_{V'}^{-1}, \tilde{Z}_{1,2,4}) - I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
&\overset{(d)}{=} H(F_{3}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2)|t}) \\
&\quad + H(F_{4}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3,4)|t}) - I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
&\overset{(e)}{\leq} H(F_{3}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3,4)|t}) - I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
&\overset{(f)}{\leq} H(F_{3}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3,4)|t}) - I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
&\overset{(g)}{\leq} H(F_{3}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3,4)|t}) - H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t}) \\
\end{align*}
\]

where (a) is due to the fact that

\[
I(\tilde{Z}_3, F_{V'} \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}) = I(\tilde{Z}_3 \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}) + I(F_{V'} \wedge \tilde{Z}_{1,2,4}|F_{V'}^{-1}, \tilde{Z}_3)
\]

(b) is due to the chain rule expansion, (c) is due to the fact that

\[
I(F_{V'} \wedge \tilde{Z}_{1,2,3,4}|F_{V'}^{-1}) \leq H(F_{V'}|F_{V'}^{-1})
\]

(d) is due to the chain rule expansion and the fact that

\[
H(F_{(1,2)|t}|F_{V'}^{-1}, \tilde{Z}_{1,2,4}) = 0
\]

by (2.4), Similarly, (e) follows from (2.4) that

\[
H(F_{4}\|F_{V'}^{-1}, \tilde{Z}_{1,2,4}, F_{(1,2,3)|t}) = 0
\]

(f) follows from the fact that conditioning cannot increase entropy, (g) is because

\[
I(F_{V'} \wedge \tilde{Z}_3|F_{V'}^{-1}) \geq I(F_{(1,2,3)|t} \wedge \tilde{Z}_3|F_{V'}^{-1}) \\
\geq I(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t}) \\
= H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t})
\]

by (2.4).

Following similar steps as above, \( c_t \) is also upper bounded by

\[
\begin{align*}
c_t &\leq H(F_{(3,4)}|F_{V'}^{-1}, \tilde{Z}_{1,2,5}, F_{(1,2)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2,5}, F_{(1,2,3,4)|t}) \\
&\quad - H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t}) \\
&\leq H(F_{(3,4)}|F_{V'}^{-1}, \tilde{Z}_{1,2,5}, F_{(1,2)|t}) - H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t})
\end{align*}
\]

Therefore, we have

\[
\begin{align*}
&\quad a_t + b_t + c_t \\
&\overset{(a)}{\leq} I(F_{(3,4,5)}|F_{V'}^{-1}, F_{(1,2)|t}) \\
&\quad + H(F_{3}\|F_{V'}^{-1}, \tilde{Z}_{1,2}, F_{(1,2)|t}) \\
&\quad + H(F_{5}\|F_{V'}^{-1}, \tilde{Z}_{1,2}, F_{(1,2,3,4)|t}) \\
&\quad + H(F_{(3,4)}|F_{V'}^{-1}, \tilde{Z}_{1,2}, F_{(1,2)|t}) - 2H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t}) \\
&\overset{(a)}{\leq} H(F_{(3,4,5)}|F_{V'}^{-1}, F_{(1,2)|t}) - H(F_{3}\|F_{V'}^{-1}, F_{(1,2)|t}) \\
&= H(F_{(4,5)}|F_{V'}^{-1}, F_{(1,2,3)|t})
\end{align*}
\]

Finally,

\[
H(F_{(4,5)}|F_{V'}) = \sum_{t=1}^{r} H(F_{(4,5)}|F_{(4,5)}^{-1})
\]

\[
\geq \sum_{t=1}^{r} (a_t + b_t + c_t)
\]

which completes the proof.

APPENDIX B
PROOFS FOR SECTION IV

1. Proof of Theorem 25

\( 1) \) Converse Proof of \( C_S: \) We first prove \( \leq \) for (4.11) by making use of the following result that directly extends the technique of the converse proof of [1, Th. 2] and [2, Th. 6]. For proving the converse result we will assume the secret key to be weakly secure, i.e., we shall assume that instead of (4.3) the secret key \( K \) only needs to satisfy

\[
\lim_{n \to \infty} \frac{1}{n} \left[ \log |K| - H(K|F, \tilde{Z}_D) \right] = 0. \tag{B.1}
\]

It is easy to see that any \( K \) satisfying (4.3) will automatically satisfy (B.1). Hence, it is enough to upper bound the secret key capacity \( C_S \) defined using \( K \) satisfying (B.1).

Lemma 38: For any \( B \subseteq V \setminus \{S,B\}, \) we have

\[
\limsup_{n \to \infty} \frac{1}{n} H(K|F, \tilde{Z}_{V \setminus \{S,B\}}) \geq H(Z_B|Z_{V \setminus \{S,B\}}) - r(B) \tag{B.2a}
\]

with \( r_i := \limsup_{n \to \infty} \frac{1}{n} \left[ \sum_{t \in [i]} H(F_{it} | F_{it}, \tilde{Z}_D) \right. \]

\[
\left. + H(\tilde{Z}_i | \tilde{Z}_D, \tilde{Z}_{i-1}, K, F) - H(U_{i}) \right]. \tag{B.2b}
\]

The inequality is satisfied with equality if \( B = V \setminus D \setminus S. \) \( \square \)
This completes the proof because, by the secrecy constraint (4.3),
\[
\lim\inf_{n \to \infty} \frac{1}{n} \log |K| \leq \lim\sup_{n \to \infty} \frac{1}{n} H(K|F, \tilde{Z}_D) = H(\tilde{Z}_D|D, S) - r(D|S)\]
by the equality case of (B.2a) with \(B = V \setminus D, S\). Moreover, 
\(r(V \setminus D, S)\) satisfies (4.13b) because, for any \(j \in A\) and \(B \subseteq V \setminus D, S\), the limit in (B.2a) is 0 by Fano’s inequality and the recoverability constraint (4.2) as \(j \in V \setminus S, B\). (Note that the constraints for \(B \ni j\) are redundant.)

**Proof (Lemma 38):** By independence of the private randomizations and the memorylessness of the private source,
\[
H(\tilde{Z}_B|\tilde{Z}_V \setminus S, B) = \sum_{i \in B} H(U_i) + nH(Z_B|\tilde{Z}_V \setminus S, B).
\]
Alternatively, since \(F\) is determined by \(\tilde{Z}_V \setminus S\), we have
\[
H(\tilde{Z}_B|\tilde{Z}_V \setminus S, B) = H(F(\tilde{Z}_V \setminus S, B)|\tilde{Z}_V \setminus S, B) = H(K, F, \tilde{Z}_B|\tilde{Z}_V \setminus S, B) - n\delta_n
\]
where \(\delta_n := \frac{1}{n} H(K|F, \tilde{Z}_V \setminus S)\) goes to 0 as \(n \to \infty\) by Fano’s inequality because \(K\) can be recovered from \((F, \tilde{Z}_V \setminus S)\) asymptotically by (4.2), due to the assumption \(S \subseteq A\) that there must be at least one vocal active user, i.e., \(A \cap (V \setminus S) \neq \emptyset\). Expanding the last entropy term \(\delta_n\) by the chain rule gives
1. \(H(F(\tilde{Z}_V \setminus S, B) + H(K|F, \tilde{Z}_V \setminus S, B)\)
2. \(= \sum_{i \in B} \sum_{i \in B} H(F_i|\tilde{F}_i, \tilde{Z}_V \setminus S, B)\)
3. \(\leq \sum_{i \in B} \sum_{i \in B} H(F_i|\tilde{F}_i, \tilde{Z}_V \setminus S, B) \leq \sum_{i \in B} \sum_{i \in B} H(F_i|\tilde{F}_i, \tilde{Z}_D)\)
4. \(= \sum_{i \in B} \sum_{i \in B} H(\tilde{Z}_i|\tilde{Z}_D, \tilde{Z}_{i-1}, K, F)\)
5. \(\leq \sum_{i \in B} \sum_{i \in B} H(\tilde{Z}_i|\tilde{Z}_D, \tilde{Z}_{i-1}, K, F)\)

where (a) is because the entropy terms for \(i \not\in B\) are zero by (2.4). Rearranging the terms give (B.2) with the desired equality condition because inequalities (b) and (c) holds with equality if \(B = V \setminus D, S\).

**2) Characterization of \(R_{CO}\):** Next, we prove the characterization of \(R_{CO}\) in (4.12). For each \(j \in A\), let
\[
\mathcal{R}'_i(\tilde{Z}_V \setminus D|S|D) := \{r(D, S) \in \mathbb{R}^{V \setminus D, S} | r(D) \geq H(\tilde{Z}_D|\tilde{Z}_V \setminus S, B, j) \forall B \subseteq V \setminus D, S\} \tag{B.3a}
\]
\[
r(B) \geq H(\tilde{Z}_D|\tilde{Z}_V \setminus S, B, j) \forall B \subseteq V \setminus D, S\)
\]
\[
\mathcal{R}'(\tilde{Z}_D|Z_j) := \{r(D) \in \mathbb{R}^D | r(B) \geq H(\tilde{Z}_D|\tilde{Z}_D, B, j) \forall B \subseteq D\} \tag{B.3b}
\]
\[
r(D) = H(\tilde{Z}_D) \forall r(D) \in \mathcal{R}'(\tilde{Z}_D) \cap \mathcal{R}'(\tilde{Z}_D),
\]
which is the maximum and minimum possible sum rates over \(\mathcal{R}(\tilde{Z}_D)\) and \(\mathcal{R}'(\tilde{Z}_D)\) respectively. An optimal solution to (4.14) exists because any \(r(D) \in \mathcal{R}(\tilde{Z}_D) \cap \mathcal{R}'(\tilde{Z}_D)\) is a feasible solution, i.e., for all \(j \in A\) and \(B \subseteq D\),
\[
r(B) = r(D) - r(D)B \geq H(\tilde{Z}_D) \forall B \subseteq V \setminus D, S
\]
satisfying the constraint (4.14b).

It remains to show that the omniscience strategy achieves \(C_2\). Consider \(r(D)\) optimal to (4.13a) and any \(r(D)\) optimal to (4.14a). Note that \(r(D)\) is \(\mathcal{R}(\tilde{Z}_D)\) by (4.14a). Then, by Proposition 39, there exists a non-negative weight vector \(\delta_D \succeq 0\) such that \(r(D) + \delta_D \in \mathcal{R}(\tilde{Z}_D) \cap \mathcal{R}'(\tilde{Z}_D)\), which is therefore in \(\mathcal{R}'(\tilde{Z}_D)\).

As a side note, although the omniscience strategy here assumes non-interactive discussion, it can be shown as in [1] that the characterization of \(R_{CO}\) remains unchanged even if interactive discussion is allowed.
By the usual source coding results [4], there exists \((F, G_D)\) at rate \(r_{V\setminus S}^{*}, \delta_D)\) such that
\[
\lim_{n \to \infty} \Pr(Z_D^* \neq \phi(F_D, G_D)) = 0
\]
in addition to satisfying the omniscience constraints (4.5). (Note that \(G_D\) is not a part of the public discussion. It is only used for the purpose of the proof, i.e., to show the additional savings in public discussion compared to (4.9).) It follows by Fano’s inequality that the l.h.s. of the secrecy constraint (4.3) can be rewritten as
\[
\lim_{n \to \infty} \frac{1}{n} \left[ \log |K| - H(K|F, Z_D^*) \right] = \lim_{n \to \infty} \frac{1}{n} \left[ \log |K| - H(K|F, G_D) \right].
\]
By [1, Lemma B.2], the r.h.s. can be made equal to 0 (satisfying (4.3)) with
\[
\lim_{n \to \infty} \frac{1}{n} \left| \log |K| \right| \geq H(Z_{V\setminus S}) - r^*(V \setminus S) - \delta(D)
\]
\[= H(Z_{V\setminus S}, D) - r^*(V \setminus D) + \left[ H(D) - r^*(D) - \delta(D) \right].\]
This achieves the r.h.s. of (4.11) as desired.

2. Proofs for Section IV-C

Proof (Proposition 28): Applying Theorem 25 to the current case \(S \subseteq A = V\), (4.11) becomes
\[
C_S = H(Z_{V\setminus S}) - R_{CO},
\]
where \(R_{CO} = \rho = \min_{r_{V\setminus S}} r(V \setminus S)\) subject to the constraints
\[
r(B) \geq H(Z_{V\setminus S}|Z_{V\setminus S} \cup B) \quad \forall B \subseteq V \setminus S : B \neq \emptyset \quad (B.5a)
\]
\[
r(V \setminus S) \geq H(Z_{V\setminus S}|Z_i) \quad \forall i \in S, \quad (B.5b)
\]
where we have used a similar argument as in the proof of Corollary 26 to derive (B.5a). Note also that the set of constraints are equivalent to the those in Corollary 27 but stated in a convenient form for the current proof. We proceed to prove (4.16a) and hence assume \(|V \setminus S| = 1\). Observe that this condition renders (B.5a) obsolete and hence using (B.4) we have
\[
C_S = H(Z_{V\setminus S}) - \max_{e \in E} H(Z_{V\setminus S}|Z_e) = a
\]

To complete the proof of Proposition 28 we consider the case when \(|V \setminus S| > 1\). Again, we shall prove this in a case by case basis. First, consider the case when (B.5b) are redundant, and hence \(R_{CO} \geq \max_{e \in E} H(Z_{V\setminus S}|Z_e)\). Also, observe that since \(R_{CO} = \min_{r_{V\setminus S}} r(V \setminus S)\), where \(r_{V\setminus S}\) is constrained by the first set of constraints in (B.5a), we have \(H(Z_{V\setminus S}) - R_{CO} = I(Z_{V\setminus S})\) using Proposition 6. Therefore, using (B.4), we have \(C_S = I(Z_{V\setminus S})\). Also, from the fact that \(R_{CO} \geq \max_{e \in E} H(Z_{V\setminus S}|Z_e)\), we have \(C_S = H(Z_{V\setminus S}) - R_{CO} \leq a\), and hence (4.16b) is satisfied. We finish the proof by looking at the remaining case, i.e., when there exists some \(i \in S\) such that (B.5b) is not redundant. An immediate consequence of this is \(R_{CO} = H(Z_{V\setminus S}|Z_i)\) and hence using (B.4) we have \(C_S = a\). Also, defining \(R_{CO}^{*} = \min_{r_{V\setminus S}} r(V \setminus S)\), where \(r_{V\setminus S}\) is constrained by (B.5a), we see that \(R_{CO} \geq R_{CO}^{*}\). Therefore, using Proposition 6, we have \(I(Z_{V\setminus S}) \geq H(Z_{V\setminus S}) - R_{CO} = C_S\). Hence, we have \(C_S = \min(a, I(Z_{V\setminus S}))\) as desired.

Proof (Theorem 29): We first consider the case when the conditions for (4.18a) hold. The proof is carried out by exactly following the same steps as in the proof of Theorem 13 with the choice \(P = \mathcal{P}_{\ast}(Z_{V\setminus S})\). This is possible as in this case \(C_S = I(Z_{V\setminus S})\) by (4.16b). Similarly, we prove the result for the case when the conditions for (4.18b) hold, by using \(C_S = I(Z_{V\setminus S} \wedge Z_i)\), for some \(i \in S^*\), which follows from (4.16a).

For the remaining case when \(|V \setminus S| > 1\) and \(a = I(Z_{V\setminus S})\), we observe using (4.16b) that every \(i \in S^*\) satisfies
\[
C_S = I_{P_{\ast}}(Z_{V\setminus S}) = I(Z_{V\setminus S} \wedge Z_i). \quad (B.6)
\]
[18, Corollary 5.3], says that there exists some \(\theta \in (0, 1)\) which satisfies \(I_{P_{\ast}}(Z_{V\setminus S} \wedge Z_i) = \theta I_{P_{\ast}}(Z_{V\setminus S}) + (1 - \theta)I(Z_{V\setminus S} \wedge Z_i)\), with \(P = \mathcal{P}_{\ast}(Z_{V\setminus S}) \cup \{i\}\). Hence, using (B.6), we have \(C_S = I_{P_{\ast}}(Z_{V\setminus S} \wedge Z_i)\) for every \(i \in S^*\). The result now follows by proceeding along the same steps as in the proof of Theorem 13, with the choice \(P = \mathcal{P}_{\ast}(Z_{V\setminus S}) \cup \{i\}\), for any \(i \in S^*\).

Proof (Theorem 30): The proof technique is similar to the proof of Theorem 15. We use the hypothesis of Theorem 30 to show that the lower bound to \(R_S\) obtained in Theorem 29 evaluates to \(R_{CO}\). This, in conjunction with the trivial upper bound \(R_S \leq R_{CO}\), gives us the result.

We first observe that the conditions in (i) imply that \(J_{D_{\mathcal{P}_{\ast}}(Z_{V\setminus S})} = H(Z_{V\setminus S})\). Hence, via (4.18a) and the inequality \(J_{W_{\mathcal{P}_{\ast}}(Z_{V\setminus S})} \geq J_{D_{\mathcal{P}_{\ast}}(Z_{V\setminus S})}\), we have \(R_S \geq H(Z_{V\setminus S}) - I(Z_{V\setminus S}) = R_{CO}\).

Next we consider the case when the conditions in (ii) hold. Therefore, there exists \(i \in S^*\) satisfying \(J_{D_{\mathcal{P}_{\ast}}(Z_{V\setminus S} \wedge Z_i)} = H(Z_{V\setminus S} \wedge Z_i) \). Hence, the lower bound to \(R_S\) in (4.18c) evaluates to \(R_{CO}\) by (4.16b) and (B.4). Therefore, we have \(R_S = R_{CO}\) as required.

Proof (Proposition 31): Choose any vocal active user \(j \in A \cap (V \setminus S)\). It is admissible to choose the secret key \(K = \theta_j(Z_j, F)\) for some function \(\theta_j\). Assume that there is a hyperedge \(e'\) such that \(\zeta(e') \subseteq S\). Then, the sequence of random variables \(X^a_{e'}\) associated with the hyperedge \(e'\) is independent of \((K, F, (X^a_{e'} | e \in E(e'))), U_{V\setminus S}\). This is because \(X^a_{e'}\) is not observed by any vocal user, including \(j\), who generate \(K, F\) entirely from \((X^a_{e'} | e \in E(e')), U_{V\setminus S}\). Similarly, it can be argued that \(X^a_{e'}\) does not play any part in recovering \(Z^a_{V \setminus S}\), as it is independent of \(X^a_{e'}\). Therefore, removing the hyperedge \(e'\) does not affect \(C_S, R_S\) and \(R_{CO}\).

Proof (Theorem 32): Proposition 31 ensures it is enough to prove the results for hypergraphs satisfying (4.19). Observe that (4.20a) follows directly from (4.18a). We only need to verify the other two scenarios.
We proceed according to a case by case basis.

Then, there exists a hyperedge $e' \in E$ that contributes to $I(Z_j \wedge Z_{(V \setminus S)\cup S}) = H(X_E)$, but not to $I(Z_j \wedge Z_{(V \setminus S)}) = H(X_E')$, i.e., $e' \in E \setminus E'$ and $E' \supseteq E$. It immediately implies that $j \notin \xi(e')$ and $\xi(e') \subseteq S$, which violates (4.19). Hence, we must have $I(Z_j \wedge Z_{(V \setminus S)\cup S}) = \alpha$, for all $j \in S^*$ and all $S' \subseteq S^* \setminus \{j\}$.

Using the above claim, we proceed to prove (4.20c). Consider any $j \in S^*$, and observe that $\alpha = I(Z_{V \setminus S} \wedge Z_j) = I_{P^*}(Z_{V \setminus S})$, using the hypothesis of (4.20c). Now, using [18, Corollary 5.3], there exists $\theta \in (0, 1)$ such that $I_{P^*}(Z_{V \setminus S}\cup j)(Z_{(V \setminus S)\cup j}) = \theta I_{P^*}(Z_{V \setminus S}) + (1 - \theta)I(Z_j \wedge Z_{V \setminus S}) = \alpha$. We can continue with this process inductively to show that $I_{P^*}(Z_{V \setminus S}\cup j)(Z_{(V \setminus S)\cup j}) = \alpha = C_S$. Using this, one can proceed along similar steps as in the proof of Theorem 13 to obtain (4.20c).

The proof of (4.20b) follows using a similar inductive argument and we omit the details.

**Proof (Theorem 33):** To begin with, we restrict our attention to hypergraphs satisfying (4.19). This is because of Proposition 31 and the fact that none of the entropy terms in (i)-(iii) are affected by the removal of some hyperedge $e$ satisfying $\xi(e) \subseteq S$.

We omit the proof of the fact that $R_S = R_{CO}$ if the required condition from (i)-(iii) hold, by noting that the proof follows from Theorem 32 by the same steps as in the proof of Theorem 30. We focus on proving the fact that $R_S = R_{CO}$ implies that the required condition from (i)-(iii) hold. We proceed according to a case by case basis.

**Case I:** $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) < \alpha$.

We assume that (i) does not hold. We will show that $R_S < R_{CO}$ if the required condition from (i)-(iii) hold, by noting that the proof follows from Theorem 32 by the same steps as in the proof of Theorem 30. We focus on proving the fact that $R_S = R_{CO}$ implies that the required condition from (i)-(iii) hold. We proceed according to a case by case basis.

**Case II:** $|V \setminus S| = 1$ or, when $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$. Here, we drop the case when $|V \setminus S| = 1$ as the condition holds by default.

Again, assume (ii) does not hold. Then, there exists a hyperedge $e' \in E$ such that $\xi(e') \subseteq (V \setminus S^*)$. We can reduce the entropy of $X_{e'}$ by some $\epsilon > 0$ small enough without affecting the secrecy capacity using decremental secret key agreement as in [11] and [12] to reduce $H(X_E)$ by some amount of $\epsilon$, $\alpha = I(Z_S \setminus S) = \alpha$ as the reduction in entropy will not affect the set $S^*$ of optimal solutions and therefore $\alpha$. In the other case $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) > \alpha$, we impose an additional constraint that $\epsilon < I(Z_{V \setminus S}) - \alpha$. Then, $\alpha$ remains unaffected after the reduction in entropy, whereas $I(Z_{V \setminus S})$ decreases by at most $\epsilon$. Thus, $C_S$ remains unchanged. Moreover, the fact that (4.19) holds implies $H(Z_{V \setminus S})$ reduces by $\epsilon$, and so does $R_{CO}$ using (B.4). Therefore, we must have $R_S < R_{CO}$ before reduction.

**Case III:** $|V \setminus S| > 1$ and $I(Z_{V \setminus S}) = \alpha$.

Assume (iii) is invalid and, hence, there exists $e' \in E$ such that $\xi(e') \subseteq C$ for some $C \in P^*(Z_{V \setminus S})$. We reduce the entropy of $X_e$ by some amount of $\epsilon > 0$. While $\alpha$ remains unaffected by the operation, the decremental secret key agreement detailed in [11] and [12] ensures that choosing $\epsilon$ sufficiently small not affect $I(Z_{V \setminus S})$ either. Thus, $C_S$ is unaffected. However, clearly $H(Z_{V \setminus S})$ reduces by $\epsilon$ and so does $R_{CO}$. Hence, $R_S < R_{CO}$ before reduction as required.

**References**

[1] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[2] A. A. Gohari and V. Anantharam, “Information-theoretic key agreement of multiple terminals—Part I,” *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[3] H. Tyagi, “Common information and secret key capacity,” *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sep. 2013.

[4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam, “On the public communication needed to achieve SK capacity in the multiterminal source model,” *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3811–3830, Jul. 2016.

[6] C. Chan and L. Zheng, “Mutual dependence for secret key agreement,” in *Proc. 44th Ann. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, Mar. 2010, pp. 1–6.

[7] T. A. Courtade and T. R. Halford, “Coded cooperative data exchange for a secret key,” *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3785–3795, Jul. 2016.

[8] M. Mukherjee and N. Kashyap, “The communication complexity of achieving SK capacity in a class of PIN models,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, Jun. 2015, pp. 296–300.

[9] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, “Secret key generation for a pairwise independent network model,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6482–6489, Dec. 2010.

[10] S. Nitinawarat and P. Narayan, “Perfect omniscience, perfect secrecy, and Steiner tree packing,” *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6490–6500, Dec. 2010.

[11] C. Chan, A. Al-Bashbashi, and Q. Zhou, “Incremental and decremental secret key agreement,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 2514–2518.

[12] C. Chan, A. Al-Bashbashi, and Q. Zhou, “Change of multivariate mutual information: From local to global,” *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 57–76, Jan. 2018.

[13] C. Chan, “The hidden flow of information,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, St. Petersburg, Russia, Jul./Aug., 2011, pp. 978–982.

[14] N. Milosavljevic, S. Pawar, S. El Rouayheb, M. Gastpar, and K. Ramchandran, “Deterministic algorithm for the cooperative data exchange problem,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, St. Petersburg, Russia, Jul./Aug. 2011, pp. 410–414.

[15] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography—Part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[16] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[17] S. El Rouayheb, A. Sprintson, and P. Sadeghiz, “On coding for cooperative data exchange,” in *Proc. IEEE Inf. Theory Workshop (ITW)*, Cairo, Egypt, Jan. 2010, pp. 1–5.

[18] C. Chan, A. Al-Bashbashi, J. B. Ebrahimi, T. Kaced, and T. Liu, “Multivariate mutual information inspired by secret-key agreement,” *Proc. IEEE*, vol. 103, no. 10, pp. 1883–1913, Oct. 2015.

[19] C. Chan. (Jun. 2008). “On tightness of mutual dependence upperbound for secret-key capacity of multiple terminals.” [Online]. Available: https://arxiv.org/abs/0805.3200.

[20] S. Fujishige, “Polyomatroidal dependence structure of a set of random variables,” *Inf. Control*, vol. 39, no. 1, pp. 55–72, 1978.


[21] R. W. Yeung, “A new outlook on Shannon’s information measures,” IEEE Trans. Inf. Theory, vol. 37, no. 3, pp. 466–474, May 1991.

[22] R. W. Yeung, Information Theory and Network Coding. New York, NY, USA: Springer, 2008.

[23] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam, “Achieving SK capacity in the source model: When must all terminals talk?” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, HI, USA, Jun./Jul. 2014, pp. 1156–1160.

[24] H. Zhang, Y. Liang, and L. Lai, “Secret key capacity: Talk or keep silent?” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Hong Kong, Jun. 2015, pp. 291–295.

[25] C. Chan, A. Al-Bashabsheh, Q. Zhou, N. Ding, T. Liu, and A. Sprintson, “Successive omniscience.” IEEE Trans. Inf. Theory, vol. 62, no. 6, pp. 3270–3289, Jun. 2016.

[26] C. Chan and T. Liu, “Clustering by multivariate mutual information under Chow–Liu tree approximation,” in Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput. (Allerton), Monticello, IL, USA, Sep./Oct. 2015, pp. 993–999.

[27] C. Chan, A. Al-Bashabsheh, Q. Zhou, T. Kaced, and T. Liu, “Info-clustering: A mathematical theory for data clustering,” IEEE Trans. Mol. Biol. Multi-Scale Commun., vol. 2, no. 1, pp. 64–91, Jun. 2016.

[28] C. Chan, A. Al-Bashabsheh, Q. Zhou, and T. Liu, “Duality between feature selection and data clustering,” in Proc. 54th Annu. Allerton Conf. Commun., Control, Comput. (Allerton), Monticello, IL, USA, Sep. 2016, pp. 142–147.

[29] A. D. Wyner, “The common information of two dependent random variables,” IEEE Trans. Inf. Theory, vol. IT-21, no. 2, pp. 163–179, Mar. 1975.

[30] W. Liu, G. Xu, and B. Chen, “The common information of N dependent random variables,” in Proc. 48th Annu. Allerton Conf. Commun., Control, Comput. (Allerton), Monticello, IL, USA, Sep. 2010, pp. 836–843.

[31] T. S. Han, “Linear dependence structure of the entropy space,” Inf. Control, vol. 29, no. 4, pp. 337–368, 1975.

[32] Q. Chen, F. Cheng, T. Liu, and R. W. Yeung, “A marginal characterization of entropy functions for conditional mutually independent random variables (with application to Wyner’s common information),” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Hong Kong, Jun. 2015, pp. 974–978.

[33] C. Chan, “Generating secret in a network,” Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Massachusetts Inst. Technol., Cambridge, MA, USA, 2010.

[34] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “Secret key agreement under discussion rate constraints,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Aachen, Germany, Jun. 2017, pp. 1519–1523.

[35] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “When is omniscience a rate-optimal strategy for achieving secret key capacity?” in Proc. IEEE Inf. Theory Workshop (ITW), Cambridge, U.K., Sep. 2016, pp. 354–358.

[36] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[37] P. Gács and J. Körner, “Common information is far less than mutual information,” Problems Control Inf. Theory, vol. 2, no. 2, pp. 149–162, Feb. 1972.

[38] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou. (Feb. 2017). “On the optimality of secret key agreement via omniscience.” [Online]. Available: https://arxiv.org/abs/1702.07429

[39] C. Chan, “Compressed secret key agreement: Maximizing multivariate mutual information per bit,” Entropy, vol. 19, no. 10, p. 545, 2017.

[40] H. G. Eggleston, Convexity. Cambridge, U.K.: Cambridge Univ. Press, 1958.

[41] A. Schrijver, Combinatorial Optimization: Polyhedra and Efficiency. New York, NY, USA: Springer, 2002.

Chung Chan received the B.Sc., M.Eng. and Ph.D. from the EECS Department at MIT in 2004, 2005 and 2010 respectively. He was a Research Assistant Professor at the Institute of Network Coding, the Chinese University of Hong Kong from 2013 to 2017. He is currently an Assistant Professor in the Department of Computer Science, City University of Hong Kong. His research interest is to develop general information measures and flow models from network information theory that are applicable to practical problems. His research topics include the development of network link models using matroids, the derivation of theoretical limits and optimal strategies for the problems of multimodal source coding, data exchange, and secret generation.

Manuj Mukherjee received the B.E. degree in Electronics and Telecommunication Engineering from Jadavpur University, Kolkata, India, in 2011, and the Ph.D. degree in Electrical Communication Engineering from the Indian Institute of Science, Bangalore, India, in 2017. Currently, he is a postdoctoral researcher at Telecom ParisTech, Paris, France. His research interests include looking at security and function computation from an information-theoretic perspective.

Navin Kashyap (S’97–M’02–SM’07) received the B.Tech. degree in Electrical Engineering from the Indian Institute of Technology, Bombay, in 1995, the M.S. degree in Electrical Engineering from the University of Missouri-Rolla in 1997, and the M.S. degree in Mathematics and the Ph.D. degree in Electrical Engineering from the University of Michigan, Ann Arbor, in 2001. From November 2001 to November 2003, he was a postdoctoral research associate at the University of California, San Diego. From 2004 to 2010, he was on the faculty of the Department of Mathematics and Statistics at Queen’s University, Kingston, Ontario. In January 2011, he joined the Department of Electrical Communication Engineering at the Indian Institute of Science, where he is currently a Professor. His research interests lie primarily in the application of combinatorial and probabilistic methods in information and coding theory. Prof. Kashyap served on the editorial board of the IEEE TRANSACTIONS ON INFORMATION THEORY during the period 2009–2014. He is at present an Associate Editor for the SIAM Journal on Discrete Mathematics.

Qiaoqiao Zhou received his B.B.A. in business administration and M.S. in electrical engineering from Beijing University of Post and Telecommunication, China, in 2011 and 2014, respectively. In 2014–2015 he was a research assistant at Institute of Network Coding, the Chinese University of Hong Kong. He is currently a Ph.D. student at Department of Information Engineering, the Chinese University of Hong Kong. His research interests include information-theoretic security and machine learning.