Secret key agreement for hypergraphical sources with limited total discussion

Chung Chan

Abstract—This work considers the problem of multiterminal secret key agreement by limited total public discussion under the hypergraphical source model. The secrecy capacity as a function of the total discussion rate is completely characterized by a polynomial-time computable linear program. Compared to the existing solution for a particular hypergraphical source model called the pairwise independent network (PIN) model, the current result is a non-trivial extension as it applies to a strictly larger class of sources and a more general scenario involving helpers and wiretapper’s side information. In particular, while the existing solution by tree-packing can be strictly suboptimal for the PIN model with helpers and the hypergraphical source model in general, we can show that incremental secret key agreement and linear network coding is optimal, resolving a previous conjecture in the affirmative. The converse is established by a single-letter upper bound on the secrecy capacity for discrete memoryless multiple sources and individual discussion rate constraints. The minimax optimization involved in the bound can be relaxed to give the best existing upper bounds on secrecy capacities such as the lamination bounds for hypergraphical sources, helper-based bound for general sources, the bound at asymptotically zero discussion rate via the multivariate Gács–Kőrner common information, and the lower bound on communication complexity via a multivariate extension of the Wyner common information. These reductions unify existing bounding techniques and reveal surprising connections between seemingly different information-theoretic notions. Further challenges are posed in this work along with a simple example of finite linear source where the current converse techniques fail even though the proposed achieving scheme remains optimal.

Index Terms—Multiterminal secret key agreement; constrained secrecy capacity; hypergraphical sources.

I. INTRODUCTION

The problem of secret key agreement by public discussion was formulated by [1, 2] where two users with correlated private observations discuss in public at unlimited rate to agree on a common secret key. The key has to be secured from a wiretapper who listens to the entire public discussion and observes some side information correlated with the users’ private observations. The fact that public discussion helps generate more secret key bits was discovered in [3]. A natural question is: What is the maximum secret key rate, called the secrecy capacity, achievable by a given public discussion rate? Equivalently, what is the minimum discussion rate, called the communication complexity, required to achieve a given secret key rate? Rate-limited public discussion was first considered in [4], which also introduced a helper who can help generate the secret key but needs not recover it. [5] extended the problem to the multiterminal case involving arbitrary numbers of users and helpers, who can be trusted or untrusted.

The secrecy capacity or communication complexity is, in general, unknown except in some special cases. For the two-user case, the capacity was characterized in [1] with unlimited one-way public discussion. With two-way interactive discussion but no wiretapper’s side information, the capacity reduces to Shannon’s mutual of the user’s private observations [1, 2]. If, in addition, that the number of rounds of interactive discussion is limited, the communication complexity that achieves the largest possible secrecy capacity was given by [6]. Subsequently, the secrecy capacity as a function of the individual discussion rates of the two users was derived in [7]. If the number of rounds is unlimited, however, these characterizations are not considered single-letter solutions as they involve optimizations over an unbounded number of auxiliary random variables, which are incomputable.

Despite the difficulty in getting a single-letter characterization of the secrecy capacity in the two-user case, the multiterminal case has been considered and resolved partially. For instance, [8, 9] characterized the capacity for the case with no discussion or at asymptotically 0 discussion rate. In the other extreme where the discussion is unlimited, the secrecy capacity was characterized in [5] when there is no wiretapper’s side information. The capacity as a function of the total discussion rate was characterized in [10] for the case without helpers and for a graphical source model called the pairwise independent network (PIN) model proposed in [11]. The capacity as a function of individual discussion rate is also characterized in [12] for the tree PIN model, and in [13, 14] for minimally connected hypergraphical sources. Other than the above cases, there are various bounds on the secrecy capacity and communication complexity [12, 15–21] for general and special source models, but exact characterizations remain unknown.

In particular, there appears no direct extension of existing solutions to cover the PIN model with helpers and hypergraphical sources that are not necessarily minimally connected. The achieving scheme for PIN model without helpers in [10, 12] used the tree-packing scheme of [11, 22], which is strictly suboptimal in achieving the secrecy capacity, even in the case with unlimited public discussion. The solution for minimally connected hypergraphical sources in [13, 14] was derived using a bound in [12] that can be loose when the PIN model has cycles.

The focus of this work is primarily on the multiterminal setting with an arbitrary number of users and helpers. The goal is to unify different bounding techniques in existing...
works and improve them to give exact single-letter capacity characterizations for a larger class of source models beyond the PIN and minimally connected hypergraphical sources. In particular, decremental secret key agreement was conjectured to be optimal for hypergraphical sources [12, 17]. The conjecture can be further generalized to the optimality of compressed secret key agreement for finite linear sources [21]. With the same linearity arguments as in [20], the conjecture implies the optimality of the linear network coding scheme [23–27] and that private randomization is not needed.

In this work, we have unified and improved existing bounding techniques to show that decremental secret key agreement is optimal for hypergraphical source. Furthermore, the secrecy capacity can communication complexity for hypergraphical sources are characterized by linear programs that are polynomial-time computable. For finite linear sources, the conjecture remains unsolved, but we give an example to illustrate the limitation of the converse result and the potential improvement. We remark that [28] also characterized the communication complexity for hypergraphical sources but under the assumption that the discussion is linear. Furthermore, [28] considered a one-shot model where the communication complexity was shown to be NP-hard to compute. In contrast, we consider an asymptotic model without assuming the discussion is linear and obtained polynomial-time computable characterizations. We also remark that there is a duality between the secret key agreement problem and the problem of generating maximum common randomness (distributed simulation) [23, Theorem 2.3]. Hence, the results for secret key agreement can translate to the results for maximum common randomness and vice versa.

The paper is organized as follows. We formulate the secret key agreement problem for general sources and hypergraphical sources in Section II. Section II gives the main results, namely an improved converse for general sources and its reduction to the exact linear programming characterizations for hypergraphical sources. Section IV explains how the converse reduces to various existing bounds on secrecy capacity and communication complexity. Section V gives an example of a finite linear source for which the converse is loose. The proofs are given in the appendix.

II. PROBLEM FORMULATION

We consider the multiterminal secret key agreement problem formulated in [5] for a multiterminal discrete memoryless source

\[ Z_V := \{Z_i \mid i \in V\} \text{ and } \tilde{Z} \]

distributed according to a given joint distribution \( P_{Z_V} \tilde{Z} \) over a possibly unbounded support set \( Z_V \times \tilde{Z} \). \( V \) is a finite set of users, \( Z_i \) is the private source of user \( i \in V \), and \( \tilde{Z} \) is the wiretapper’s side information.

For secret key agreement, every user \( i \in V \) observes an \( n \) i.i.d. sequence \( \{Z_{i1}\ldots Z_{in}\} := \{Z_1\ldots Z_m\} \) and generates a private and possibly continuous random variable \( U_i \) independent of the source, i.e.,

\[ P_{U_V|Z_V} = \prod_{i \in V} P_{U_i}. \]  

Then, the users engage in an interactive public discussion where some user \( i_j \in V \) at round \( j \in \{1, \ldots, r\} \) of the discussion reveals in public a finitely valued message

\[ \tilde{F}_j := f_j(U_{i_j}, Z_{i_j}^{n}, \tilde{F}^{j-1}), \]

namely a deterministic function of the accumulated knowledge of user \( i_j \), which includes the private randomization \( U_{i_j} \), source \( Z_{i_j}^{n} \), and all the previous discussion \( \tilde{F}^{j-1} \). For notational simplicity, we define

\[ F_i := \{\tilde{F}_j \mid j \in \{1, \ldots, r\}, i_j = i\}, \]

\[ F := F_V, \]

namely the entire discussion by user \( i \) and by all users respectively.

After the public discussion, a subset \( A \subseteq V \) of the users, called the active users, wants to agree on a secret key \( K \) secured against a wiretapper observing \( \tilde{Z}^n \), the entire discussion \( F \), and the source \( Z_V^n \) of a subset \( D \subseteq V \setminus A \) of users called the untrusted helpers. (\( V \setminus A \) is called the set of helpers, where \( V \setminus A \) is the set of trusted helpers.) More precisely, a sequence in \( n \) of \( U_V \), \( F \) and \( K \) is a secret key agreement scheme if there exist decoding functions \( \phi_i \) for \( i \in A \) such that

\[ \lim_{n \to \infty} \Pr\{K = \phi_i(U, Z_i^n, F) \forall i \in A\} = 1 \]

\[ \lim_{n \to \infty} \log|K| - H(K|F, Z_D^n) = 0, \]

where \( K \) denotes a finite set of possible secret key values. The prior condition (3) is called the recoverability constraint and the latter one (4) is called the secrecy (and uniformity) constraint.

A secret key rate \( r_K \in \mathbb{R}_+ \) is said to be achievable by the public discussion rates \( r_V := \{r_i \mid i \in V\} \in \mathbb{R}_+^V \) if and only if there exists a secret key agreement scheme \( (K, F) \) satisfying the above conditions (3) and (4), and the rate constraints

\[ r_K \leq \liminf_{n \to \infty} \frac{1}{n} \log|K| \]

\[ r_i \geq \limsup_{n \to \infty} \frac{1}{n} \log|F_i| \quad \forall i \in V, \]

where \( F_i \) denotes the set of possible messages by user \( i \).

Denotes the set of achievable rate tuple \((r_K, r_V)\) by \( \mathcal{R}_V^{A,D}[Z_V|\tilde{Z}] \). The secrecy capacity is the maximum achievable key rate denoted by

\[ C_S^{V,A,D}[Z_V||\tilde{Z}](r_V) := \sup\{r_K \in \mathbb{R}_+ \mid (r_K, r_V) \in \mathcal{R}_V^{A,D}[Z_V||\tilde{Z}]\}, \]

\[ C_S^{V,A,D}[Z_V||\tilde{Z}](R) := \sup\{r_K \in \mathbb{R}_+ \mid (r_K, r_V) \in \mathcal{R}_V^{A,D}[Z_V||\tilde{Z}], r(V) \leq R\}, \]

for \( r_V \in \mathbb{R}_+^V \) and \( R \in \mathbb{R}_+ \), where, for notational convenience, we define for \( B \subseteq V \)

\[ r(B) := \sum_{i \in B} r_i. \]
It is easy to see that the secrecy capacity is non-decreasing in the discussion rates. The communication complexity as a function of the key rate \( r_K \) is defined as
\[
R_S^{V,A,D}|Z_V\|\tilde{Z} (r_K) := \inf \left\{ R \in \mathbb{R}_+ \mid C_S^{V,A,D}|Z_V\|\tilde{Z} (R) = C_S^{V,A,D}|Z_V\|\tilde{Z} (\infty) \right\},
\]
which is simply the inverse of \( C_S^{V,A,D}|Z_V\|\tilde{Z} (R) \). In the rest of the paper, we will omit the dependency on \( V, A, D, Z_V, \tilde{Z} \) and write
\[
\mathcal{P}, C_S(r_V), C_S(R), R_S(r_K)
\]
for the case without untrusted helper \((D = \emptyset)\) nor wiretapper’s side information \((\tilde{Z} = 0)\) unless otherwise specified. We will also write
\[
C_S = \lim \inf_{R \to \infty} C_S(R) \quad \text{(9)} \\
R_S = \lim \sup_{r_K \to C_S} R_S(r_K) \quad \text{(10)}
\]
respectively for the \textit{unconstrained secrecy capacity} with unbounded discussion rate, and the communication complexity to attain the unconstrained secrecy capacity.

Consider a hypergraph \((V, E, \xi)\) with vertex set \( V \), edge set \( E \) and the edge function \( \xi : E \to 2^V \setminus \{\emptyset\} \), where \( \xi(e) \) denotes the set of vertices incident on an edge \( e \in E \). A hypergraphical source is defined with respect to such a hypergraph as \([23, 29]\)
\[
Z_i = (X_e \mid i \in \xi(e)) \quad \text{for} \ i \in V \quad \text{(11a)}
\]
where \( X_E \) is a given random vector and \( X_e \)’s are independent random variables called the edge \((\text{random})\) variables with bounded supports. In other words, each user gets to observe a subset of the independent edge variables. The model covers the pairwise independent network (PIN) model \([11, 22]\) as a special case when exactly two users observe each edge variable, i.e., \( |\xi(e)| = 2 \), and so the hypergraph reduces to a graph. One may also consider a hypergraphical source model with wiretapper’s side information where
\[
\tilde{Z} = X_{\tilde{E}} \quad \text{(11b)}
\]
for some given subset \( \tilde{E} \subseteq E \).

### III. MAIN RESULTS

All the converse results in this paper are based on the following single-letter upper bound on the secrecy capacity. The bound applies to general sources and allows for trusted helpers, i.e., with \( D = \emptyset \) but \( V \setminus A \) possibly non-empty.

\begin{theorem}

The secrecy capacity \((6)\) as a function of discussion rate \( r_V \in \mathbb{R}^V \) is upper bounded as follows:
\[
C_S(r_V) \leq \sup_{W, r_V'} I(W \wedge Z_V) - r'(V) \quad \text{(12a)}
\]
\[
= \sup_{W} \min_{\lambda \in \Lambda} \left\{ I(W \wedge Z_V) - r(V) \right\} - \sum_{B \supseteq A} \lambda(B) \left[ I(W \wedge Z_B|Z_V \setminus B) - r(B) \right], \quad \text{(12b)}
\]
where

- the maximization in the first expression \((12a)\) is over the choices of an auxiliary random variable \( W \) (or its distribution \( P_W(Z_V) \), more specifically) and a real vector \( r_V' \in \mathbb{R}^V \) subject to the constraints
\[
r'_{\Lambda} (B) \geq I(W \wedge Z_B|Z_V \setminus B) \quad \forall B \supseteq A \quad \text{(13a)}
\]
\[
r'_{\Lambda} \leq r_i \quad \forall i \in V; \quad \text{(13b)}
\]
- the minimization in the second expression \((12b)\) is over the choice of a set function \( \lambda : \{B \subseteq V \mid B \supseteq A\} \to \mathbb{R}_+ \) satisfying
\[
\sum_{B \supseteq A : i \in B} \lambda(B) \geq 1 \quad \forall i \in V. \quad \text{(14)}
\]
\end{theorem}

\textbf{Proof} See Appendix A.

An important simplification is to consider the total discussion rate constraint instead of the individual rates. The above bound translates directly to the following bound on the secrecy capacity for a given total discussion rate.

\begin{corollary}

The secrecy capacity \((7)\) for \( R \geq 0 \) are upper bounded as follows:
\[
C_S(R) \leq \sup_{W, r(V)} \{ I(W \wedge Z_V) - r(V) \mid r(V) \leq R \}
\]
\[
= \sup_{W, r(W) \leq R} I(W \wedge Z_V) - \rho(W) \quad \text{(15a)}
\]
\[
\rho(W) := \max_{\lambda \in \Lambda} \sum_{B \supseteq A} \lambda(B) I(W \wedge Z_B|Z_V \setminus B) \quad \text{(15b)}
\]
\end{corollary}

\begin{theorem}

The corresponding lower bound on the communication complexity \((8)\),
\[
R_S(r_K) \geq \inf_{W, I(W \wedge Z_V) - r_K \geq \rho(W)} I(W \wedge Z_V) - r_K \quad \text{(20)}
\]
for any given secret key rate \( r_K \geq 0 \).
\end{theorem}

\textbf{Proof} See Appendix B.

\textbf{Note} that the above bounds involve an auxiliary random variable \( W \), an optimal solution of which exists by standard support lemma \([30]\) if the support of the random source is finite. It is also straightforward to argue that the upper bounds on the secrecy capacity are non-decreasing, concave, and continuous in the discussion rates. The two expressions \((12a)\) and \((12b)\)
and (12b)) for the upper bound (12) are related by the linear programming duality [31], where the minimization over \( \lambda \) is the dual of the maximization over \( r_V' \). \( \lambda(B) \) is the Lagrangian multiplier for the constraints on \( r_V' \) in (13).

It is instructive to compare \( r_V' \) to the feasible rate of communication for omniscience [5] in

\[
\mathcal{R}_C = \{ r_V \in \mathbb{R}^V | r(B) \geq H(Z_B|Z_V \setminus B) \forall B \subseteq V : B \nsubseteq A \}. \tag{21a}
\]

\[
r(B) \geq H(Z_B|Z_V \setminus B) \forall B \subseteq V : B \nsubseteq A \}. \tag{21b}
\]

The above corresponds to the set of public discussion rate tuple such that each user can recover the entire source after the discussion, i.e., attain omniscience. Suppose the source \( Z_V \) has finite support. Then, the region must be non-empty. The constraints in (13a) play a similar role as the Slepian-Wolf constraints in (21b) above. In particular, the two sets of constraints are the same if \( W = Z_V \) and \( r_V' = r_1 \). This connection can be observed similarly in the bounds for total discussion rate instead of individual discussion rate. In particular, with \( W = Z_V, \rho(W) \) defined in (17) becomes the smallest rate of communication for omniscience [5]

\[
R_{CO} = \min_{r_V \in \mathcal{R}_C} r(V) \tag{22a}
\]

\[
= \max_{\lambda \in \Lambda} \sum_{B \subseteq A} \lambda(B)H(Z_B|Z_V \setminus B) \tag{22b}
\]

where the last equality is again by the linear programming duality. With \( \rho(W) = R_{CO} \) and assuming \( Z_V \) has finite support, the bound (15b) on secrecy capacity becomes (16), which is the unconstrained secrecy capacity characterized in [5] as

\[
C_S = H(Z_V) - R_{CO}
\]

\[
= \min_{\lambda \in \Lambda} I_\lambda(Z_V), \tag{23b}
\]

where \( I_\lambda \) is the information measure defined in (18). The last equality means that the bound (16) is tight when \( Z_V \) has finite support. The expression is non-negative as expected because by the Shearer Lemma (see [32, Lemma D.1] or [23, 33])

\[
I_\lambda(Z_V) \geq 0 \tag{24}
\]

with equality if \( Z_i \)'s are mutually independent. In the case without helpers, i.e., \( A = V \), (23b) can be further simplified to the following multivariate mutual information as shown in [29, 34, 35]:

\[
I(Z_V) = \min_{p \in \Pi'(V)} \frac{1}{|P|} D(p_{Z_V} \parallel \prod_{C \in P} p_{Z_C}) \tag{25a}
\]

\[
:= \inf \{ \gamma \in \mathbb{R} | \forall p \in \Pi'(V), H(Z_V) - \gamma = \sum_{C \in P} H(Z_C) - \gamma \} \tag{25b}
\]

where \( \Pi'(V) \) is the set of partitions of \( V \) into at least two non-empty disjoint sets. The first expression (25a) was given as an upper bound on \( C_S \) in [5]. It can be obtained from (18) with

\[
\lambda(B) = \begin{cases} 
\frac{1}{|P|-1} & V \setminus B \in \mathcal{P} \\
0 & \text{otherwise}. 
\end{cases} \tag{26}
\]

for any partition \( \mathcal{P} \) of \( V \). The constraint in the second expression (25b) is the constrained residual independence relation given in [35, 36], which means that \( I(Z_V) \) is the smallest amount of shared information removal of which leads to independence.

The bounds on the secrecy capacity and communication complexity can be shown to be tight for the hypergraphical sources as follows:

**Theorem 2** For hypergraphical sources defined in (11a), the secrecy capacity (7) and communication complexity (8) are equal to the upper bound (15b) and lower bound (20) respectively, which can be simplified further by setting

\[
W = (Q_{E}, X'_{E}) \tag{27a}
\]

\[
X'_{e} = \begin{cases} 
X & Q_e = 1 \\
0 & Q_e = 0 
\end{cases} \text{ for } e \in E \tag{27b}
\]

\[
\text{and } Q_e \text{'s are independent bits independent of the source with distribution}
\]

\[
\frac{p_{Q_{E}}(Q_e)}{p_{Q_{E}|X_{E}}(Q_e)} = \prod_{e \in E} \text{Bern}(\frac{Q_e}{P(E_e)}) \tag{27c}
\]

for some vector \( x_V \in \mathbb{R}^V \).

**PROOF** See Appendix C.

**Corollary 2** For hypergraphical sources, \( R, r_K \geq 0 \),

\[
C_S(R) = \max \{ x(E) - r(V) | r(V) \leq R \}
\]

\[
r(B) \geq x(E(B)) \forall B \subseteq V : B \nsubseteq A \tag{28a}
\]

\[
= \min \{ x(E) - r_K | 0 \leq x_e \leq H(X_e) \forall e \in E \}
\]

\[
= \max \{ x(E) - \rho | \rho \leq R \}
\]

\[
\rho = \max_{\lambda \in \Lambda} \sum_{B \subseteq A} \lambda(B)x(E(B)) \tag{28b}
\]

\[
\leq x_e \leq H(X_e) \forall e \in E
\]

\[
R_S(r_K) = \min \{ x(E) - r_K | 0 \leq x_e \leq H(X_e) \forall e \in E \}
\]

\[
\{ x(E) - \sum_{B \subseteq A} \lambda(B)x(E(B)) \geq r_K \} \tag{29}
\]

where we define \( x(E') := \sum_{e \in E'} x_e \) for \( E' \subseteq E \) as usual and

\[
E(B) := \{ e \in E | \{ e \} \subseteq B \} \text{ for } B \subseteq V \tag{30}
\]

namely, the set of edges that are incident only on nodes within \( B \). The linear programs above can be solved in polynomial-time.

**PROOF** See Appendix D.

The theorem is proved by showing that the bounds (15b) and (20) on the secrecy capacity can be achieved by the decremental secret key agreement scheme in [16, 37]. The linear programs in the corollary are obtained by evaluating the bounds (15b) and (20) explicitly with the optimal solution choice of the auxiliary random variable \( W \) in (27).
The idea of decremental secret key agreement is to reduce the randomness of the source $Z_V$ by eliminating some randomness of each edge variable, leading to a reduced source $Z'_V$, and then generate the secret key via omniscience of the reduced source, i.e., achieving the unconstrained secrecy capacity of $Z'_V$. More formally, the reduced source is

$$Z'_i := (X'_e | i \in \xi(e)) \quad \text{for } i \in V$$

where $X'_e$ and $Q_e$ are as defined in (27) for some vector $x_V \in \mathbb{R}^V$. Each user $i \in V$ can privately reduce their source $Z_i$ effectively to $Z'_i$ by keeping only the first $\frac{h(X_e)}{h(Z)}$ fraction of the $n$ i.i.d. samples of $X_e$ for each edge $e \in E$ with $i \in \xi(e)$. An immediate generalization of decremental secret key agreement to general sources beyond hypergraphic sources is the \textit{compressed secret key agreement} in [21], where the reduced source $Z'_i$ can be chosen as arbitrary processing of $Z_i$ with a time sharing variable $Q$, i.e.,

$$H(Z'_i|Z_i, Q) = 0 \quad P_{Q|Z_i} = P_Q.$$ (32)

The secret key rate $C_S[Z'_V|Q]$ is therefore achievable by a discussion of rate $R_{CO}[Z'_V|Q]$, where, similar to the conditional entropy $H(Z'_V|Q)$, $C_S$ and $R_{CO}$ evaluated at $Z'_V|Q$ means conditioning on $Q$, i.e., with distribution $P_{Z'_V|Q}(\cdot|Q)$ as the source, and then take expectations with respect to $Q$.

The optimality of decremental secret key agreement resolved the conjecture in [17] that decremental secret key agreement is optimal and also the conjecture in [10] that linear network coding (discussion) is optimal. The idea of secret key agreement by linear network coding can be found in [24–27, 38, 39]. A straightforward extension of the results to the case with untrusted helpers and wiretapper’s side information is as follows:

\textbf{Proposition 1} \textit{In the case with untrusted helpers $(D \neq \emptyset)$ and wiretapper’s side information (11b), we have}

$$C^V_{S,D}[Z_V||W](R) = C^V_{S,D\emptyset}[Z'_V](R) \quad \text{where}$$

$$Z'_i := (X_e | e \in E \setminus \tilde{E}, \quad i \in \xi(e), D \cap \xi(e) = \emptyset) \quad \text{for } i \in V \setminus D,$$

which is obtained from $Z_i$ by removing the edge variables observed by the untrusted helpers and wiretappers. \hfill \Box

\textbf{Proof} Note that $\geq$ for (34) holds because $Z'_i$ can be obtained from $Z_i$ for $i \in V$, and $Z'_{V\setminus D}$ is independent of $(\cdot)Z_{D,\tilde{Z}}$. To explain the reverse inequality, note that the capacity does not decrease by turning the wiretapper into an untrusted helper, i.e.,

$$C^V_{S,D}(Z_V||W)(R) \leq \min_{\lambda \in \Lambda^*} I_{\lambda}(Z_V|W) \quad \text{where}$$

$$\min_{\lambda \in \Lambda^*} I_{\lambda}(Z_V|W) = R_{CO} \quad \text{as desired by (23)}. \hfill \Box$$

\textbf{IV. REDUCTION TO VARIOUS CONVERSE RESULTS}

In this section, we will show that the bounds in Theorem 1 and Corollary 1 unify various exiting converse results. First of all, by the result of [5] that the upper bound (16) on $C_S$ can be achieved via communication for omniscience at the smallest rate, it is straightforward to show that, for any smallest omniscience rate tuple $r_V \in \mathbb{R}_{CO} : r(V) = R_{CO}$ and sum rate $R \geq R_{CO}$, the upper bounds (12), (15b), and (16) are tight, equal to the unconstrained secrecy capacity given by (23). Furthermore, $W = Z_V$ is optimal to the maximizations in the upper bounds (12) and (15b). Indeed, if $W = Z_V$ is also optimal to the minimization in the lower bound (20), then the lower bound is also tight:

\textbf{Proposition 2} \textit{For $Z_V$ with finite support, $R_S = R_{CO}$, i.e., the communication for omniscience scheme in [5] for secret key agreement achieves $R_S$, if $W = Z_V$ is an optimal solution to the minimization in the lower bound (20) on the communication complexity for some $r_K \in [0, C_S]$. In particular, this holds if $Z_V$ has finite support and}

$$\min_{W: I_X(Z_V|W)=0, \forall X \in \Lambda^*} I(W \wedge Z_V) = H(Z_V)$$ (37)

where $\Lambda^*$ is the set of optimal solutions $\lambda$ to (16). \hfill \Box

\textbf{Proof} Suppose $W = Z_V$ is optimal to (20). Then, (20) becomes

$$R_S(r_K) \geq H(Z_V) - r_K \geq H(Z_V) - \min_{\lambda \in \Lambda} I_{\lambda}(Z_V) \quad \text{by (16)}$$

$$R_S(r_K) \geq R_{CO} \quad \text{by (23b)}.$$ Equality holds as desired since $R_S \leq R_{CO}$ by the omniscience scheme for secret key agreement in [5].

Next, we show that (37) implies $W = Z_V$ is optimal to (20) with $r_K = C_S$ as follows. By (20)

$$R_S(C_S) \geq \inf_{W: I_X(Z_V|W)\geq C_S} I(W \wedge Z_V) - C_S$$

(a) \hfill \inf_{W: \min_{\lambda \in \Lambda} I_{\lambda}(Z_V)} I(W \wedge Z_V) - C_S \geq\hfill \min_{\lambda \in \Lambda} I_{\lambda}(Z_V)$$

(b) \hfill \inf_{W: I_X(Z_V|W)=0, \forall X \in \Lambda^*} I(W \wedge Z_V) - C_S.$$ (38)

(a) is obtained by rewriting the constraint by (65) and $C_S(R) = \min_{\lambda \in \Lambda} I_{\lambda}(Z_V)$ by (23), which in turn holds as $R_{CO} < \infty$ for $Z_V$ with finite support. (b) is because, for any $\lambda \in \Lambda^*$, the constraint implies that

$$I_{\lambda}(Z_V) - I_{\lambda}(Z_V|W) \geq I_{\lambda}(Z_V), \quad \text{or equivalently}$$

$$I_{\lambda}(Z_V|W) = 0.$$ Finally, if (37) holds, we have

$$R_S(C_S) \geq H(Z_V) - C_S = R_{CO}$$ as desired by (23). \hfill \Box

The above result covers the sufficient condition in [19, 32].

More precisely, the sufficient condition in [32] is in terms of
the multivariate Wyner common information defined below for a fractional partition $\lambda$ as
\[
C_{W,\lambda}(Z_V) := \inf_{W} I(W \wedge Z_V) \quad \text{such that} \quad I_{\lambda}(Z_V | W) = 0.
\]
(38) can be rewritten as $C_{W,\lambda}(Z_V) = H(Z_V)$, which is the sufficient condition in [32] with helpers.

In the other extreme where the discussion rate has to be 0, the upper bounds on the secrecy capacity are also tight, which cover the result in [9] with helpers.

**Proposition 3** With $r'_{V} = 0$ and $R = 0$, the secrecy capacity upper bounds (12) and (15b) are tight and simplifies to the Gács–Körner common information
\[
J_{\text{GK}}(Z_{A}) := \max \{ H(G) | G < \infty, \ H(G|Z_i) = 0 \ \forall i \in A \}.
\]
(40a)
Furthermore, the optimal solution $G_{\lambda}$, called the maximal common function of $Z_i$ for $i \in A$, is an optimal solution for $W$ in (12) and (15b).

**Proof** With $r_{V} = 0$, (13a) and (13b) implies that an optimal $W$ must satisfy
\[
0 = I(W \wedge Z_B | Z_V \backslash B) \ \forall B \subseteq V : B \nsubseteq A = I(W \wedge Z_V \backslash \{i\} | Z_i) \ \forall i \in A
\]
where the last equality is obtained by setting $B = V \backslash \{i\}$. By the double Markov inequality [40, Problem 16.25],
\[
I(W \wedge Z_V | G) = 0
\]
for the optimal solution $G$ to (40). It follows that
\[
I(W \wedge Z_V) \leq I(W, G \wedge Z_V) = I(G \wedge Z_V) + H(W \wedge Z_V | G) = H(G),
\]
which implies by (12a) that
\[
C_{S}(r_{V}) \leq H(G) = J_{\text{GK}}(Z_{A}).
\]
Equality holds as desired as we can use the entire randomness of $G$ for the secret key without any discussion. More precisely, by [5, Lemma B.1], a key rate of $H(G) \geq r_{V} = H(G)$ is achievable.

The constraint (40a) requires $G$ to have finite support. If we set $W = G$, then $r(W) = 0$ in (17) by the constraint (40b) that $G$ is a function of $Z_i$ for any $i \in A$, and hence the name common function. The secrecy capacity upper bound (15b) then becomes $H(G) = J_{\text{GK}}(Z_{A}).$ The bound is achievable intuitively because $G$ is a common function of the active users and so, even with no discussion, a common secret key can be extracted from $G$ at rate $H(G)$.

Other than the two extreme cases with unlimited or 0 discussion rate, the secrecy capacity upper bound (12) strictly improves the existing bounds for multiterminal secret key agreement. In particular, it implies the following result that not only covers the bound in [12, Theorem 4.1] for general sources but also extends it to the case with helpers.

**Proposition 4** We have $C_{S}(r_{V}) \geq r_{K}$ only if
\[
r(S) \geq \frac{1}{\sum_{B \in \mathcal{R}} \lambda'(B) - I[r_{K} - I_{\lambda}(Z_{V} \backslash S)]
\]
(41)
For all $S \subseteq V : |A \setminus S| \geq 2$ and $\lambda' : \{B \subseteq V \setminus S : B \nsubseteq A \setminus S \} \rightarrow \mathbb{R}_{+}$ satisfying
\[
\sum_{B \nsubseteq A \setminus S} \lambda'(B) = 1,
\]
(42)
i.e., $\lambda'$ is a fractional partition of $V \setminus S$.

**Proof** See Appendix E.

It is instructive to consider the condition on $r_{K}$ where the bound becomes trivial for a given choice of $S$, i.e., $r(S) \geq 0$. Since the factor $\sum_{B \in \mathcal{R}} \lambda'(B)$ is strictly positive, the bound is trivial only if
\[
r_{K} \leq \min_{\lambda'} I_{\lambda}(Z_{V} \backslash S).
\]
The condition is rather intuitive because, by (23b), the expression on the right is the unconstrained secrecy capacity when $S$ is removed or not allowed to discuss. (41) is called the helper-set bound because it gives how much discussion (help) users in $S$ need so that users in $V \setminus S$ can share a key at a rate beyond their capacity.

Although the bound (41) looks quite different from the original bound (12b), it can be derived directly from the original bound by exchanging the maximization and minimization and then restricting the set of possible $\lambda$ appropriately. The bound in [12, Theorem 4.1] for the case without helpers, i.e., $A = V$, can be obtained from (41) with
\[
\lambda'(B) = \begin{cases} \frac{1}{|\mathcal{P}|-1}, & V \setminus B \in \mathcal{P} \setminus \{S\} \\ 0, & \text{otherwise.} \end{cases}
\]
(43)
for any partition $\mathcal{P}$ of $V \setminus S$.

For hypergraphical sources, since the characterizations of the secrecy capacity in (11) is tight, it covers the lamination bounds in [10]. The following result unifies the lamination bounds:

**Proposition 5** For hypergraphical sources and $R \geq 0$,
\[
0 \leq C_{S}(R) - H(X_{E' \backslash E'}) \leq \left( \frac{1}{\max_{\lambda \in \Lambda} \alpha(\lambda)} - 1 \right) R
\]
(44)
where
\[
E' := \{ e \in E | \xi(e) \nsubseteq A \}
\]
(45)
\[
\alpha(\lambda) := \begin{cases} \min_{e \in E'} \sum_{B \nsubseteq A : \xi(e) \subseteq B} \lambda(B), & H(X_{E'}) \neq 0 \\ 1, & \text{otherwise.} \end{cases}
\]
(46)
Equality holds if $R \leq \min_{e \in E'} H(X_{e})$.

**Proof** See Appendix F.

Note that the upper bound is linear in $R$, and the slope can be bounded as follows.
Proposition 6 For hypergraphical sources, the slope of $R$ in the upper bound (44) can be bounded as follows:

$$0 \leq \frac{1}{\max_{\lambda \in A} \alpha(\lambda)} - 1 \leq \min_{d} \left\{ \frac{|d|}{|A|} - d, 1 \right\}$$

where

$$d := \max_{e \in E'} |\xi(e)|$$

(47)

denotes the maximum degree of the edges in $E'$. Furthermore, the bounds in (47) can be achieved with equality for some hypergraphs.

PROOF See Appendix G.

To reduce the upper in (44) to the EP bound in [10], consider as in [10] the case $A = V$, $H(X_{E'}) \neq 0$ and $H(X_{E'} \setminus B) = 0$. Let

$$\lambda_{P}(B) = \begin{cases} \frac{1}{|P|} & V \setminus B \in P \\ 0 & \text{otherwise} \end{cases}$$

for any partition $P$ of $V$ with $|P| > 1$. Then,

$$\alpha(\lambda_{P}) = \min_{e \in E'} \sum_{B \in E' | A \xi(e) \subseteq B} \lambda_{P}(B)$$

$$= \frac{1}{|P| - 1} \min_{e \in E'} \left\{ |V \setminus B| \in P | \xi(e) \subseteq B \right\}$$

$$= \frac{1}{|P| - 1} \min_{e \in E'} \left\{ |P| - |C \in P | \xi(e) \cap C \neq \emptyset | \right\}$$

$$= 1 - \max_{e \in E'} \left\{ |C \in P | \xi(e) \cap C \neq \emptyset | \right\}$$

Substituting the above into (44) gives the EP bound [10, Theorem 4.1].

Next, to reduce to the VP bound in [10], define for $u_{V} \in \mathbb{R}_{+}^{V}$

$$\lambda_{u_{V}}(B) = \begin{cases} \frac{u_{i}}{u(V)} & i \in V, B \in \{i\}, V \setminus \{i\} \\ 0 & \text{otherwise} \end{cases}$$

Then,

$$\alpha(\lambda_{u_{V}}) = \min_{e \in E'} \sum_{B \in E' | A \xi(e) \subseteq B} \lambda_{u_{V}}(B)$$

$$\geq \min_{e \in E'} \sum_{i \in \xi(e), \theta \in V \setminus \{i\}} \frac{u_{i}}{u(V)}$$

$$= \min_{e \in E'} \sum_{i \in V \setminus \xi(e)} \frac{u_{i}}{u(V)}$$

$$= 1 - \max_{e \in E'} \frac{u(\xi(e))}{u(V)}$$

Applying the above to (44) In particular, with $u_{V}$ chosen to be the solution to

$$\tau = \max_{u_{V} \in \mathbb{R}_{+}^{V} : u(\xi(e)) \leq 1, \forall e \in E} u(V),$$

we have

$$\alpha(\lambda_{u_{V}}) \geq 1 - \frac{1}{\tau}$$

Applying the above into (44) gives the VP bound [10, Theorem 4.3].

V. CHALLENGES

For hypergraphical sources, it is plausible that the upper bound (12) of $C_{S}(r_{V})$ in Theorem 1 may also tight. In this work, we have only shown that the corresponding upper bound (15b) of $C_{S}(R)$ in Corollary 2 under total discussion rate constraint instead of individual rate constraints is tight.

If we consider more general sources beyond the hypergraphical sources, however, the bound (15b) on $C_{S}(R)$ may be loose. In this section, we give an example of a finite linear source where the bound (20) on $R_{S}$ is loose, and so is (15b). Nevertheless, it remains plausible that compressed secret key agreement and linear network coding is optimal for general finite linear sources.

Consider $A = V = \{1, 2, 3, 4, 5\}$ and

$$Z_{1} = X_{a}$$

$$Z_{2} = X_{b}$$

$$Z_{3} = X_{c}$$

$$Z_{4} = (X_{a}, X_{b}, X_{d})$$

$$Z_{5} = (X_{a}, X_{b}, X_{c} \oplus X_{d})$$

where $X_{a}, X_{b}, X_{c}, X_{d}$ are uniformly random and independent bits, and $\oplus$ denotes the XOR or binary addition operation.

Proposition 7 $R_{S} = 3 > 2 \geq \rho(C_{S})$ for (49) and so the bound (20) on the communication complexity is loose.

PROOF It was shown in [19] that $C_{S} = 1$ and $R_{S} = R_{CO} = 3$. It remains to show that the lower bound (20) is at most 2, i.e.,

$$\inf_{W : I(W \wedge Z_{V}) - C_{S}} I(W \wedge Z_{V}) - C_{S} \geq 2$$

To do so, it suffices to show that a feasible solution $W$ to the L.H.S. is

$$W = (X_{a}, X_{b}, X_{c})$$

because then the bound is at most

$$I(Z_{V} \wedge W) - C_{S} = H(X_{a}, X_{b}, X_{c}) - 1 = 2$$

desired.

It remains to show the feasibility, i.e., the following constraint holds,

$$I(W \wedge Z_{V}) - \rho(W) \geq C_{S}.$$  

Note that $I(W \wedge Z_{V}) = H(X_{a}, X_{b}, X_{c}) = 3$, $C_{S} = 1$, and $\rho(W) = \min_{r':(13a)} r'(V)$ by linear programming duality, it suffices to show that

$$\min_{r':(13a)} r'(V) \leq 2.$$  

In particular, we will argue that a feasible solution with $r'(V) \leq 2$ is

$$r' = \begin{cases} 1 & i \in \{4, 5\} \\ 0 & i \in \{1, 2, 3\}. \end{cases}$$

More precisely, we will argue that the constraint (13a) that

$$r'(B) \geq I(W \wedge Z_{B}|Z_{V \setminus B}) \ \forall B \subseteq V.$$  

We can divide all the cases of $B$ as follows:
• 4 \not\in B \text{ and } 5 \not\in B. Then,
\begin{equation}
I(W \wedge Z_B | Z_{V \setminus B}) \leq H(W | Z_4, Z_5) = 0
\end{equation}
and so the constraint holds trivially as \( r_i' \geq 0 \) for all \( i \in V \).

• 4 \not\in B \text{ or } 5 \not\in B \text{ but not both. Then,}
\begin{equation}
I(W \wedge Z_B | Z_{V \setminus B}) \leq \max_{i \in \{1,2,3\}} H(W | Z_i) \leq 2
\end{equation}
\begin{equation}
r(B) \geq \min\{r_4, r_5\} = 1
\end{equation}
Since and so the constraint holds.

• \{4,5\} \subseteq B \text{ but } 1 \not\in B \text{ or } 2 \not\in B \text{ or } 3 \not\in B. Then,
\begin{equation}
I(W \wedge Z_B | Z_{V \setminus B}) \leq \max_{i \in \{1,2,3\}} H(W | Z_i) \leq 2
\end{equation}
\begin{equation}
r(B) \geq r_4 + r_5 = 2
\end{equation}
and so the constraint holds.

This completes the proof. ■

APPENDIX

A. Proof of Theorem 1

We first derive (12b) from (12a). By the linear programming duality, we can rewrite (12a) as
\begin{equation}
\max_{W} \min_{\lambda, \mu_V} I(W \wedge Z_V) - \sum_{B \supseteq A} \lambda(B) I(W \wedge Z_B | Z_{V \setminus B}) + \sum_{i \in V} \mu_i r_i \geq 0
\end{equation}
where \( \lambda : \{ B \subseteq V \mid B \supseteq A \} \rightarrow \mathbb{R}_+ \) and \( \mu_V \in \mathbb{R}_+^V \) are subject to the constraint
\begin{equation}
\sum_{B \supseteq A : i \in B} \lambda(B) - \mu_i = 1 \quad \forall i \in V.
\end{equation}
The above constraint holds if and only if
\begin{equation}
\lambda \in \tilde{A}
\end{equation}
\begin{equation}
\mu_i = \sum_{B \supseteq A : i \in B} \lambda(B) - 1,
\end{equation}
which implies
\begin{equation}
\sum_{i \in V} \mu_i r_i = \sum_{i \in V} \sum_{B \supseteq A : i \in B} [\lambda(B) - 1] r_i
\end{equation}
\begin{equation}
= \sum_{B \supseteq A} \lambda(B) r(B) - r(V).
\end{equation}
Substituting (54) into (51) gives (12b), and we need only impose (52) but not (53) as (12b) does not depend on \( \mu_V \).

To prove (12a), we first consider the case without randomization. More precisely, let \( C_S^{NR}(r_V) \) be the secrecy capacity (6) but with no randomization, i.e., with (1) replaced by \( U_V = 0 \). We want to the that \( C_S^{NR}(r_V) \) is bounded by (12a).

For \( i \in V \), let
\begin{equation}
r_i' := \frac{1}{n} \sum_{1 \leq j \leq r_{ij} = i} H(\tilde{F}_j | \tilde{F}_{j'}) \end{equation}
It follows that
\begin{equation}
r_i' \leq \frac{1}{n} \sum_{1 \leq j \leq r_{ij} = i} H(\tilde{F}_j | \tilde{F}_{j'} \mid j' \leq j, i' = i)
\end{equation}
\begin{equation}
= \frac{1}{n} H(F_i)
\end{equation}
\begin{equation}
r_i' \leq r_i + \delta_n,
\end{equation}
where the first inequality is because conditioning reduces entropy; the last two steps are by (2b) and respectively (5b) for some \( \delta_n \rightarrow 0 \) as \( n \rightarrow 0 \). Furthermore, for \( B \subseteq V \),
\begin{equation}
r'(B) \geq \frac{1}{n} \sum_{i \in B} \sum_{1 \leq j \leq r_{ij} = i} H(\tilde{F}_j | \tilde{F}_{j} \mid B, Z_{V \setminus B})
\end{equation}
\begin{equation}
= \frac{1}{n} \sum_{i \in V} \sum_{1 \leq j \leq r_{ij} = i} H(\tilde{F}_j | \tilde{F}_{j} \mid B, Z_{V \setminus B})
\end{equation}
\begin{equation}
= \frac{1}{n} H(F | Z_{V \setminus B})
\end{equation}
where the first inequality is again because conditioning reduces entropy; the second equality is because the terms in the summation is 0 for \( i \in V \setminus B \) by the definition (2a) of \( \tilde{F}_j \). For \( B = V \), the first inequality holds with equality and so
\begin{equation}
r'(V) = \frac{1}{n} H(F).
\end{equation}
Next, we single-letterize the key rate and discussion rate as follows. Let
\begin{equation}
W_j := (K, F, Z_{V \setminus j}^{-1})
\end{equation}
and \( J \) be a random variable uniformly distributed over \( \{1, \ldots, n\} \) and independent of all other random variables. By the secrecy constraint (4),
\begin{equation}
\log|K| \leq H(K | F) + n \delta_n
\end{equation}
\begin{equation}
\leq H(K | F) + n \delta_n
\end{equation}
\begin{equation}
= n \sum_{j=1}^{n} I(K, F | Z_{V \setminus j})
\end{equation}
\begin{equation}
= n \sum_{j=1}^{n} I(K, F, Z_{V \setminus j}^{-1} | Z_{V \setminus j})
\end{equation}
\begin{equation}
= n I(W_j \wedge Z_{V \setminus j})
\end{equation}
\begin{equation}
= I(W_j \wedge Z_{V \setminus j}) - r'(V) + 2 \delta_n
\end{equation}
for some \( \delta_n \rightarrow 0 \) as \( n \rightarrow 0 \). (a) is because \( H(K, F) = I(K, F \wedge Z_{V \setminus j}) + H(K, F | Z_{V \setminus j}) \). (b) is by the recoverability constraint (3) and Fano’s inequality while (c) is by (57), (d) is because \( I(Z_{V \setminus j}^{-1} | Z_{V \setminus j} | K, F) = 0 \) by the memorylessness of the random source \( Z_{V \setminus j} \). (e) follows from the definition (58) of \( W_j \) and \( J \).
Similarly, by (3) and Fano’s inequality,

\[
H(F | Z_i^\perp | B) \geq \frac{H(F, K | Z_i^\perp | B)}{n} - n\delta_n
\]

for some \( \delta_n \to 0 \) as \( n \to 0 \). (f) is by (56). (g) follows from (e) while (h) follows from the same argument for (e). (60) follows from (56).

Since (55), (59), and (60) holds for any secret agreement scheme \((K, F)\), we have the desired bound (12a) on \( C_{SNR}^{|r_V|} \) by setting \( n \to \infty \) and noting that \( P_{Z_{ij}} = P_{Z'} \).

It remains to extend the bound (12a) to the general case with randomization (1) where \( U_V \) not necessarily deterministic. Let

\[
Z'_i := (U_i, Z_i) \quad \text{for } i \in V.
\]

We have

\[
C_S[Z_i](r_V) \leq C_{SNR}^{|r_V|}[Z'_i](r_V)
\]

because a secret key agreement scheme with randomization for \( Z_i \) is also a secret key agreement scheme with no randomization but for \( Z'_i \). It suffices to show that the R.H.S. is upper bounded by (12).

Applying the bound (12b) with the source \( Z'_i \) instead of \( Z_i \) for the secrecy capacity with no randomization, we have

\[
C_{SNR}^{|r_V|}[Z'_i](r_V) \leq \max_{W} \min_{\lambda \in \Lambda} I(W \wedge Z'_i) - r(V) - \sum_{B \geq A} \lambda(B) \left[ I(W \wedge Z'_B | Z'_V \setminus B) - r(B) \right].
\]

It suffices to show that the above bound is upper bounded by (12b), i.e., the bound above remains valid after replacing \( Z'_i \) by \( Z_i \). In particular, we will show that

\[
I(W \wedge Z'_i) - \sum_{B \geq A} \lambda(B) I(W \wedge Z'_B | Z'_V \setminus B) \leq I(W \wedge Z'_i) - \sum_{B \geq A} \lambda(B) I(W \wedge Z_B | Z_V \setminus B).
\]

Consider \( V = \{1, \ldots, m\} \) without loss of generality and define

\[
\tilde{r}_i := I(W \wedge U_i | U^{i-1}, Z_V).
\]

It follows that

\[
\tilde{r}(B) = \sum_{i \in B} I(W \wedge U_i | U^{i-1}, Z_V) \geq \tilde{r}(B) \quad \text{by (63)}
\]

where the inequality holds with equality if \( B = \emptyset \). This is because \( H(U_i | U^{i-1}, Z_V) = H(U_i | U^{i-1}, U_V \setminus B, Z_V) \) by the independence assumption (1), and \( H(U_i | U^{i-1}, Z_V, W) \geq H(U_i | U^{i-1}, U_V \setminus B, Z_V, W) \) with equality if \( B = \emptyset \). It follows that

\[
I(W \wedge Z_B' | Z_V') = I(W \wedge U_B, Z_B' | U_V \setminus B, Z_V') + \tilde{r}(B).
\]

Again, the inequalities above holds with equality if \( B = \emptyset \).

Applying (64) to the L.H.S. of (62) and subtract the resulting lower bound from the R.H.S. of (62), we have

\[
\text{L.H.S. of (62)} - \text{R.H.S. of (62)} \geq \sum_{B \geq A} \lambda(B) \left[ \tilde{r}(B) - \tilde{r}(V) \right] = \sum_{i \in V} \sum_{B \geq A, i \in B} \lambda(B) \tilde{r}(B) - \tilde{r}(V) \geq \tilde{r}(V) - \tilde{r}(V) = 0,
\]

which implies (62) as desired and therefore completes the proof.

\[\text{B. Proof of Corollary 1}\]

We first derive the bound (16) on the unconstrained capacity by (15b). By the definition 18 of \( I_{\Lambda} \),

\[
I_{\Lambda}(Z_V) - I_{\Lambda}(Z_V | W) = H(Z_V) - \sum_{B \geq A} H(Z_B | Z_V \setminus B) - H(Z_V | W) + \sum_{B \geq A} H(Z_B | Z_V \setminus B, W) = I(W \wedge Z_V) - \sum_{B \geq A} \lambda(B) I(W \wedge Z_B | Z_V \setminus B).
\]
Hence, by (15b), for $R \geq 0$,
\[ C_S(R) \leq \sup W I(W \wedge Z_V) - \rho(W) \]
\[ = \sup W \min _{\lambda} H(Z_V) - \sum _{B \subseteq A} H(Z_B|Z_{V \setminus B}) \]
\[ \leq \sup W \min _{\lambda} I_{\lambda}(Z_V) - I_{\lambda}(Z_V|W) \]
\[ \leq \min _{\lambda} I_{\lambda}(Z_V) \]
which gives (16) as desired since the bound does not depend on $R$.

Next, we derive the upper bounds (15a) and (15b) on $C_S(R)$ from the upper bound (12) on $C_S(r_V)$ as follows: For $R \geq 0$. By (7),
\[ C_S(R) = \sup \{ C_S(r_V)|r(V) \leq R \} \]
\[ \leq \sup \{ I(W \wedge Z_V) - r'(V)|r(V) \leq R, (13) \} \]
\[ \leq \sup \{ I(W \wedge Z_V) - r'(V)\rho(V) \leq R, (13b) \} \]
\[ = \sup \{ I(W \wedge Z_V) - \min \{ r'(V)|r(V) \leq R, (13b) \} \} \]
\[ \geq \sup \{ I(W \wedge Z_V) - \rho(W) \rho(W) \leq R \}, \]
which gives (15b) as desired. (b) also gives (15a). (a) is by (12). (b) is because (13b) and $r(V) \leq R$ imply $r'(V) \leq R$. (c) is because it is optimal to choose $r'_V$ to minimize $r'(V)$. (d) is by the linear programming duality and the definition (17) of $\rho(W)$.

Finally, we can derive the lower bound (20) on $R_S(r_K)$ from (15b) as follows: By (8),
\[ R_S(r_K) = \inf \{ R \geq 0|C_S(R) \geq r_K \} \]
\[ = \inf \{ R \geq 0|I(W \wedge Z_V) - \rho(W) \geq r_K, \rho(W) \leq R \} \]
\[ = \inf \{ I(W \wedge Z_V) - \rho(W)|I(W \wedge Z_V) - \rho(W) \geq r_K \} \]
\[ = \inf \{ I(W' \wedge Z_V) - r_K|I(W' \wedge Z_V) - \rho(W') = r_K \} \]
which implies (20) as desired. (e) is by (15b). (f) is obtained by setting $R = \rho(W)$ without loss of optimality. (g) is because, for any feasible $W$ to (f), we also have a feasible $W'$ to (g) and vice versa. E.g., given $W$, one can choose
\[ W' = \begin{cases} (1, W) & Y = 1 \\ (0, 0) & Y = 0 \end{cases} \]
where $Y$ is an indicator random variable independent of $(Z_V, W)$ with $I(W' \wedge Z_V) = \epsilon$. Note that
\[ I(W' \wedge Z_V) = \epsilon I(W' \wedge Z_V) \]
\[ \rho(W') = \epsilon \rho(W) \]
and so the condition in (g) can be satisfied with some $\epsilon \in [0, 1]$ as desired. This completes the proof of Corollary 1.

C. Proof of Theorem 2

In this section, we show that the upper bound (15b) on the secrecy capacity is tight for hypergraphical sources. Indeed, we show that the lower bound (20) on communication complexity is tight by showing that the following sufficient condition for tightness holds for hypergraphical sources.

Lemma 1 The lower bound (20) on communication is tight for all $r_K \in [0, C_S]$ if there exists an optimal solution $W$ to (20) in the form
\[ W = (Q, Z_V') \]
\[ I(Q \wedge Z_V') \]
\[ H(Z'_V|Q) = 0 \]
\[ \forall i \in V \]
\[ H(Z'_B|Z'_{V \setminus B}, Q) = H(Z'_B|Z_{V \setminus B}, Q) \]
\[ \forall B \subseteq A. \]

Furthermore, compressed secret key agreement [21] is optimal in achieving $R_S(r_K)$ and therefore $C_S(R)$ (15b) for $R \geq 0$.

PROOF Consider any optimal solution $W$ to (20) satisfying the condition (66). We will show that
\[ I(W \wedge Z_{V \setminus B}|Q) = H(Z_{V \setminus B}|Q) \]
\[ \forall B \subseteq V. \]

Then, the lower bound (20) can be written as
\[ I(W \wedge Z_V) - \rho_K \geq \rho(W) \]
\[ \geq \max _{\lambda \in \Lambda} \sum _{B \subseteq A} \lambda(B) I(W \wedge Z_B|Z_{V \setminus B}) \]
\[ = H(Z'_V|Q) - I_A(Z'_V|Q) \]
\[ \geq R_S(r_K) \]

which is the desired reverse inequality of the bound (20). (a) follows from the constraint on $W$ in (20). (b) is by the definition (17) of $\rho(W)$. (c) is obtained by rewriting
\[ I(W \wedge Z_B|Z_{V \setminus B}) = I(W \wedge Z_V) - I(W \wedge Z_{V \setminus B}) \]
\[ = H(Z'_V|Q) - H(Z'_V|Q) \]
\[ = H(Z'_B|Z'_{V \setminus B}, Q) \]
\[ \sum _{B \subseteq A} I(W \wedge Z_B|Z_{V \setminus B}) = H(Z'_V|Q) - I_A(Z'_V|Q) \]

where the second equality is by (67) and the last equality is by the definition (18) of $I_A$. (d) is because the R.H.S. of (c) is the discussion rate achievable by the compressed secret key agreement scheme in [21, Theorem 3] to attain a key rate of
\[ \min _{\lambda \in \Lambda} I_A(Z'_V|Q) \geq H(Z'_V|Q) - I(W \wedge Z_V) + \rho_K = \rho_K. \]

where the first inequality is by (c) and the second equality is by (67).

It remains to show (67) as follows. For $B \subseteq V$,
\[ I(W \wedge Z_{V \setminus B}) = I(Z'_V, Q \wedge Z_{V \setminus B}) \]
\[ = I(Z'_V \wedge Z_{V \setminus B}|Q) + I(Q \wedge Z_{V \setminus B}) \]
\[ = H(Z'_{V \setminus B}|Q) + I(Z_B \wedge Z_{V \setminus B}|Q, Z'_V) \]
\[ = H(Z'_{V \setminus B}|Q) \]
\[ \geq 0 \]

\[ = I(H(21, 33).}
as desired where the last equality is because
\[
I(Z_B' \land Z_{V \setminus B}|Q, Z_{V \setminus B}') = H(Z_B'|Q, Z_{V \setminus B}') - H(Z_B'|Q, Z_{V \setminus B}', Z_{V \setminus B}) = H(Z_B'|Q, Z_{V \setminus B}) \quad \text{by (66d)} \quad = H(Z_B'|Q, Z_{V \setminus B}) \quad \text{by (66c)}
\]
This completes the proof.

Note that \( W \) defined in (27) satisfies (66) with \( Z' \) defined as in (31). In particular,
\[
H(Z_B'|Z_{V \setminus B}, Q) = H(Z_B'|Z_{V \setminus B}, Q) = H(X_{E(B)}')|Q)
\]
where \( E(B) \) is defined in (30) as the set of edges that are incident only on nodes within \( B \). By the above lemma, it suffices to show that \( W \) defined in (27) is an optimal solution to the lower bound (20).

For simplicity, we rewrite the lower bound (20) as \( H(Z_V) - r_K - T \) where
\[
T := \max\{H(Z_V|W)|I(W \land Z_V) - \rho(W) \geq r_K \forall \lambda \in \Lambda\}
\]

Since the above maximization share the same set of solutions \( W \) as that of the lower bound (20), it suffices to show that \( W \) defined in (27) is optimal to the above maximization.

We further rewrite \( T \) without changing the set of optimal \( W \) below:
\[
T := \max\{H(Z_V|W)|I(W \land Z_V) - \rho(W) \geq r_K \forall \lambda \in \Lambda\}
\]

where \( E(\cdot) \) is defined in (30), and
\[
\alpha(\lambda) := I_\lambda(Z_V) - r_K + (\sum_{B \supseteq A} \lambda(B) - 1)T.
\]

- (a) is obtained by rewriting the constraint in (69) as \( r_K \leq I_\lambda(Z_V) - I_\lambda(Z_V|W) \forall \lambda \in \Lambda \).

because \( I(W \land Z_V) - \rho(W) = \min_{\lambda \in \Lambda} I(W \land Z_V) - \sum_{B \supseteq A} \lambda(B)I(W \land Z_B|Z_{V \setminus B}) = I_\lambda(Z_V) - I_\lambda(Z_V|W) \text{ by (65)} \).  

- (b) is obtained by expanding \( I_\lambda(Z_V|W) \) by its definition (18).

- (c) is because any optimal solution \( W \) to (b) is feasible to (c). To explain \( \geq \) for (c), suppose to the contrary that there exists a solution \( W \) to (c) with \( H(Z_V|W) > T \). Then, that solution is also feasible to (b) because the constraint of (c) with \( T < H(Z_V|W) \) implies the constraint in (b), which is the desired contradiction since the maximum in (b) equals \( T \).

- (d) is because \( Z_{V \setminus B} = X_{E(V \setminus B)}'. \) Note that the additional constraints in (d) but not (c) hold trivially as the edge variables have bounded supports.

It remains to argue that \( W \) defined in (27) is an optimal solution to (d). More precisely, we show that this choice of \( W \) achieves the maximum given by the linear program
\[
T' := \max\{y(E) \mid 0 \leq y_e \leq H(X_e) \forall e \in E\} \quad \text{(71a)}
\]
\[
\sum_{B \supseteq A} \lambda(B)y(E(V \setminus B)) \leq \alpha(\lambda) \forall \lambda \in \Lambda \}
\]

where \( y(E') := \sum_{e \in E} y_e \) for \( E' \subseteq E \) as usual.

- (e) is to show \( T \leq T' \), consider the dual of the linear program in (e), i.e.,
\[
T' = \min_{\mu : E \rightarrow \mathbb{R}_+} \sum_{e \in E} \mu(e)H(X_e) + \sum_{\lambda \in \Lambda} \mu(\lambda)\alpha(\lambda) \text{ such that}
\]
\[
\mu(e) + \sum_{\lambda \in \Lambda} \mu(\lambda) \sum_{B \supseteq A} \lambda(B)H(X_E(B)|W) \leq \alpha(\lambda) \forall \lambda \in \Lambda \}
\]

For any optimal solution \( \mu \), since \( H(X_{E'})|W \) is submodular in \( E' \subseteq E \), i.e.,
\[
H(X_{E_1}|W) + H(X_{E_2}|W) \geq H(X_{E_1 \setminus E_2}|W) + H(X_{E_1 \cup E_2}|W) \forall E_1, E_2 \subseteq E,
\]
we have by Edmonds’ greedy algorithm (see [10, Lemma A.1]) that, for any solution \( W \) to (d),
\[
T = H(X_E|W) \leq \sum_{e \in E} \mu(e)H(X_e|W)
\]

\[
+ \sum_{\lambda \in \Lambda} \mu(\lambda)\sum_{B \supseteq A} \lambda(B)H(X_E(B)|W) \leq \alpha(\lambda) \quad \text{by (71)}
\]

- (f) is to show \( T \geq T' \), consider any optimal solution \( y_E \) to (71) and define \( W \) by (27) with
\[
x_e := H(X_e) - y_e \quad \forall e \in E.
\]

The above definition of \( W \) is valid because (71a) implies \( x_e/H(X_e) \in [0,1] \), which is a valid probability \( P_{Q_e} \) in (27c). For \( E' \subseteq E \),
\[
H(X_{E'}|W) = H(X_{E'}|Q_e, X_e')
\]
\[
= \sum_{e \in E'} H(X_e|Q_e, X_e') = \sum_{e \in E'} H(X_e|Q_e) - H(X_e'|Q_e)
\]

\[
= y(E')
\]

The first equality is by (27a) that \( W = (Q_e, X_e') \). The second equality is by the independence of \((Q_e, X_e'|X_e)\) for \( e \in E \), which follows from (27b) and (27c). The third equality is by the fact that \( H(X_e'|X_e, Q_e) = 0 \) by (27b). The last equality is by the definition (73) of \( y_e \).
It follows that the constraint in (d) holds, i.e., for all \( \lambda \in \Lambda \),
\[
\sum_{B \supseteq A} \lambda(B) \cdot H(X_{E(V \setminus B)} | W) \leq \alpha(\lambda)
\]
by (71b). By the feasibility of \( W \) to (d),
\[
T \geq H(X_E | W) = y(E) = T'
\]
as desired. The first equality is by (74) and the last is by the optimality of \( y_E \) to (71).
This completes the proof.

D. Proof of Corollary 2

With the definition (11) of \( W \) and the definition (31) of \( Z_V' \), we have
\[
I(W \land B; Z_{V \setminus B}) = I(W \land Z_{V'} - I(W \land Z_{V \setminus B})
\]
\[
(\text{a}) \quad H(Z_V') - H(Z_{V \setminus B})
\]
\[
= H(Z_{V \setminus B}) - Q
\]
\[
(\text{b}) \quad H(Z_{V \setminus B})
\]
\[
= \sum_{e \in E(B)} H(X_e)
\]
\[
(\text{d}) \quad x(E(B))
\]
where (a) is by (67), (b) is by (68), (c) is by (27b), and (d) is by (27c).

Applying the above equality to the capacity upper bound (15a) and (15b) gives (28a) and (28b) respectively. Similarly, (29) follows from (20).

By the ellipsoid method [31], to show that the linear programs are polynomial-time solvable, it suffices to show that the following separation oracle for (28a) is,
\[
0 \leq \max\{R - r(V)\},
\]
\[
\min_{x_e, e \in E} \min_{x_e, e \in E} \min_{x_{A \subseteq V \setminus \{i\}}} r(B) - x(E(B))
\]
In particular, in the last expression, \( \min_{i \in A} \min_{B \subseteq V \setminus \{i\}} \) is equivalent to \( \min_{B \subseteq V : B \supseteq A} \). It is straightforward to verify that the above inequality holds if and only if \( (r_{V}, x_{E}) \) is a feasible solution to (28). It suffices to show that the last minimization
\[
\min_{B \subseteq V \setminus \{i\}} r(B) - x(E(B))
\]
is polynomial-time solvable despite having exponentially many constraints. To argue this, note that by (75)
\[
r(B) - x(E(B)) = \sum_{i \in B} r_i - H(Z_V') - H(Z_{V \setminus B} | Q),
\]
which is submodular in \( B \) by the submodularity of entropy [41]. Hence, (76) is a submodular function minimization over a lattice family, namely the boolean lattice, which is known to be strongly polynomial-time solvable [42]. This completes the proof.

E. Proof of Proposition 4

Consider \( S \subseteq V : |A \setminus S| \geq 2 \) and fractional partition \( \lambda' := \{ B \supseteq V \setminus S : B \supseteq A \setminus S \} \rightarrow \mathbb{R}_+ \) of \( V \setminus S \) as stated in the proposition. To prove the necessary condition (41) for \( C_S(r_V) \geq r_K \) and \( r_V \in \mathbb{R}_+^V \), it suffices to show the following upper bound
\[
C_S(r_V) \leq I_{\Lambda}(Z_{V \setminus S}) + (\Delta - 1)r(S)
\]
where
\[
\Delta := \sum_{B \supseteq A \setminus S} \lambda'(B).
\]
In particular, we will show that the above bound is given by the upper bound (12b) with \( \lambda \in \Lambda \) defined in terms of \( \lambda' \) as follows:
\[
\lambda(B) = \begin{cases} \lambda'(B \setminus S) & B \subseteq V : B \supseteq S \\ 0 & \text{otherwise}. \end{cases}
\]
where \( \lambda \in \text{barA} \), i.e., (14) holds, because
\[
\sum_{B \supseteq A \setminus S : i \in B} \lambda'(B) - 1 \quad i \in V \setminus S
\]
\[
= 0 \quad i \in V \setminus S
\]
\[
\Delta - 1 \quad \text{otherwise, by (78b)}
\]
\[
\geq 0.
\]
The last inequality is because, for any \( i \in V \setminus S \), we have
\[
\Delta \geq \sum_{B \supseteq A \setminus S : i \in B} \lambda(B) = 1.
\]
Note that the upper bound (12b) remains a valid upper bound for any given choice of \( \lambda \), i.e.,
\[
C_S(r_V) \leq \sum_{B \supseteq A} \lambda(B) \cdot (I(W \land Z_B) | Z_{V \setminus B}) + \sum_{B \supseteq A \setminus S} \lambda(B) \cdot (r(B) - r(V))
\]
With the choice of \( \lambda \) given by (79),
\[
\sum_{B \supseteq A} \lambda(B) \cdot (I(W \land Z_B) | Z_{V \setminus B})
\]
\[
= \sum_{B \supseteq A \setminus S} \lambda'(B) \cdot (I(W \land Z_B) | Z_{V \setminus B})
\]
\[
= \Delta I(W \land Z_S | Z_{V \setminus S}) + \sum_{B \supseteq A \setminus S} \lambda'(B) I(W \land Z_B | Z_{V \setminus S} | B),
\]
where the last equality is by (80).
where the last equality is again by (80).

\( 1 - 2 = I(^{(W \land Z_V)} + 2) \geq 0 \)

\( = I(W \land Z_V) + 1 \)

\( = \frac{(1 - \Delta - 1)I(W \land Z_V|Z_V)}{I(W \land Z_V|Z_V)} + \sum_{B \in \mathcal{B}, A \in \mathcal{B}} \lambda'(B) - (W \land Z_B|Z_V) \leq \frac{I(X|Z_V) - I(X|W)}{I(X|Z_V)} \quad \text{by Shearer Lemma (see (24)).} \)

Hence, \( 1 - 2 + 3 \) can be upper bounded by (78), which completes the proof.

### F. Proof of Proposition 5

Consider the characterization (28b) of \( C_S(R) \). It is optimal to set

\[ x_e = H(X_e) \quad \forall e \in E \setminus E' \]

because \( \rho \) does not depend on the above \( x_e \)'s as \( \xi(e) \geq A \) for \( e \in E \setminus E' \). (28b) can be rewritten as

\[ C_S(R) - H(X_{E \setminus E'}) = \max \{ x(E') - \rho | \rho \leq R \} \quad \text{(81a)} \]

\[ \rho = \max_{A \in \mathcal{A}} \sum_{B \in \mathcal{B}} \lambda(B)x(E(B)) \quad \text{(81b)} \]

\[ 0 \leq x_e \leq H(X_e) \quad \forall e \in E' \}. \quad \text{(81c)} \]

The above maximization is at least 0, for instance, by choosing \( x_e = 0 \) for all \( e \in E' \). This implies the first inequality in (44) as desired. It remains to show the second inequality.

Consider the case \( H(X_{E'}) = 0 \) and so \( \alpha = 1 \) by definition (70). Then, in (28b), we must have \( x(E') = \rho = 0 \) because \( x(E(B)) \leq x(E') \leq H(X_{E'}) = 0 \) for all \( B \subseteq V \). Hence, the maximum in (81) is 0, which implies (44) as desired since \( \alpha = 1 \) by the definition (70).

Consider the remaining case \( H(X_{E'}) \neq 0 \) and any optimal solution \( x_{E'} \) and \( \rho \) to (81) such that \( \rho > 0 \). To show that the choice of optimal solution is possible, note that any feasible solution satisfies

\[ x(E') \geq \sum_{B \in \mathcal{B}} \lambda(B)x(E(B)) \quad \forall e \in E' \in \mathbb{R}^E, \lambda \in \Lambda \quad \text{(82)} \]

by the Shearer Lemma. (See (24) and (77).) Suppose to the contrary that any optimal solution must have \( \rho = 0 \). By (81b), we must have \( x_e = 0 \) for all \( e \in E' \) which implies \( x(E') - \rho = 0 \). This is a contradiction because it is possible to choose \( x_e > 0 \) for some \( e \in E' \) as \( H(X_{E'}) \neq 0 \), and such choice is also optimal as \( x(E') - \rho \geq 0 \) by (82).

Next, with the optimal solution \( x_{E'} \) and \( \rho > 0 \), (81) becomes

\[ C_S(R) - H(X_{E_{E'}}) \leq x(E') - \rho \]

\[ \leq \left[ \frac{1}{\rho/E'} - 1 \right] \rho \]

with equality if \( \rho = R \). It suffices to show \( \frac{1}{\rho/E'} \geq \alpha(\lambda) \), which gives the second inequality in (81). By (81b),

\[ \frac{\rho}{E'} = \max_{\lambda \in \Lambda} \sum_{B \in \mathcal{B}} \lambda(B)x(E(B)) \]

\[ = \max_{\lambda \in \Lambda} \sum_{B \in \mathcal{B}} \lambda(B)p(E(B)) \]

where the last equality is obtained by setting

\[ p(e) = \frac{x_e}{\rho/E'} \quad \forall e \in E' \quad \text{(83)} \]

\[ p(E') = \sum_{e \in E'} p(e) \quad \forall e \in E' \subseteq E'. \]

Note that \( p \) is a probability distribution over \( E' \) since \( p(E') = 1 \) and \( p(e) \in [0, 1] \) for \( e \in E' \) by (81c). Let \( \mathcal{P}(E') \) be the set of all possible distributions over \( E' \). Then,

\[ \frac{\rho}{E'} \geq \min_{\rho \in \mathcal{P}(E')} \max_{\lambda \in \Lambda} \sum_{B \in \mathcal{B}} \lambda(B)E[I\{\xi(e) \subseteq B\}] \]

\[ = \max_{\lambda \in \Lambda} \min_{\rho \in \mathcal{P}(E')} \left[ \sum_{B \in \mathcal{B}: \xi(e) \subseteq B} \lambda(B) \right] \]

which, together with (a), gives (81) as desired. In (b), \( I\{\xi(e) \subseteq B\} \) corresponds to the indicator random variable that is equal to 1 if and only if the event \( \xi(e) \subseteq B \) happens, and so the expectation is \( P_e(E(B)) \) by the definition (30) of \( E(B) \). The inequality (b) holds with equality if \( P_e = p \) defined in (83) in terms of \( x_{E'} \) is an optimal solution. (c) is by the minmax theorem, since the objective function is linear in both \( P_e \) and \( \lambda \) over compact convex sets \( \mathcal{P}(E') \) and \( \Lambda \) respectively, (d) is because the expectation over \( e \) is no smaller than the minimum over \( e \in E' \). The last equality is by the definition (70) of \( \alpha(\lambda) \).

Finally, consider proving the equality condition. If \( R = 0 \), the inequalities in (44) holds with equality trivially. Similarly, if \( \alpha(\lambda) \geq 1 \), then \( \alpha(\lambda) - 1 \leq 0 \) and so the inequalities in (44) must hold with equality. Consider the remaining case

\[ \alpha(\lambda) < 1 \forall \lambda \in \Lambda \quad \text{(84)} \]

\[ H(X_e) > R > 0 \quad \forall e \in E'. \quad \text{(85)} \]

We first argue that the constraint \( x_e \leq H(X_e) \) in (81b) can be removed without changing the maximization in (81), i.e.,

\[ C_S(R) - H(X_{E \setminus E'}) = \max \{ x(E') - \rho | \rho \leq R \} \]

\[ = \max_{\lambda \in \Lambda} \sum_{B \in \mathcal{B}} \lambda(B)x(E(B)) \quad \text{(86)} \]

which differs from (81) in the last constraint. Suppose to the contrary that one can have a feasible solution to the above with
\[ x' \in H(X_{\varepsilon'}) \text{ for some } \varepsilon' \in \varepsilon \]. Then, with for some partition \( \{B_1, B_2\} \) of \( V \setminus \xi(e') \) such that \( B_i \supseteq A \) for \( i \in \{1, 2\} \), define
\[
\lambda'(B) = \begin{cases} 1 & B = \xi(e'), B_1, B_2 \\ 0 & \text{otherwise} \end{cases}
\]
which is a fraction partition in \( \Lambda \). It follows from the definition of \( \rho \) and the constraint \( x_{\varepsilon'} \geq H(X_{\varepsilon'}) \) that
\[
\rho \geq \lambda'(\xi(e')) x_{\varepsilon'} \geq H(X_{\varepsilon'}) > R
\]
which is the desired contradiction.

Next, we argue that the constraint \( \rho \leq R \) in (86) must be tight for the optimal solution. Suppose to the contrary that the constraint is slack. Then, (86) simplifies to
\[
\begin{aligned}
C_\varepsilon(R) - H(X_{\varepsilon'}) &= \max_{x_{E'} \in \mathbb{R}^{E'}} x(E') \\
&\quad - \max_{\lambda \in \Lambda} \sum_{B \supseteq A} \lambda(B)x(E(B)) \quad (87)
\end{aligned}
\]
where the last inequality is because
\[
1 > \max_{\lambda \in \Lambda} \alpha(\lambda) = \min_{P_\varepsilon \in \mathcal{P}(E')} \max_{\lambda \in \Lambda} \sum_{B \supseteq A} \lambda(B)E[\{\xi(e) \subseteq B\}]
\]
\[
= \min_{x_{E'} \in \mathbb{R}^{E'}} \max_{\lambda \in \Lambda} \sum_{B \supseteq A} \lambda(B)x(E(B))
\]
where the first is by (eq:LB:eq1), the second equality is by (c) and (d), and the last equality is by rewriting \( P_\varepsilon = p \) defined in (83). Now, given any feasible solution \( x_{E'} \) to (87), \( 2x_{E'} \) is a strictly better solution, and so the maximum in (87) must be unbounded, contradicting the fact that (81) is bounded by \( H(X_{\varepsilon'}) \).

Altogether, for any optimal solution \( x_{E'} \) and \( \rho = R > 0 \), (a) holds with equality as \( \rho = R \), and
\[
\begin{aligned}
\frac{\rho}{x(E')} &= \min_{x_{E'} \in \mathbb{R}^{E'}} \max_{\lambda \in \Lambda} \sum_{B \supseteq A} \lambda(B)x(E(B)) \\
&= \max_{\lambda \in \Lambda} \alpha(\lambda),
\end{aligned}
\]
i.e., (b) also holds with equality. This completes the proof.

**G. Proof of Proposition 6**

The first inequality in (47) follows immediately from (44) with any \( R > 0 \). Equality holds trivially if \( E' \in E(C_1) \cup E(C_2) \) for some bipartition \( \{C_1, C_2\} \) such that \( C_i \cap A \neq 0 \) for all \( i \in \{1, 2\} \). This is because one can show that \( \max_{\lambda \in \Lambda} \alpha(\lambda) = 1 \) with \( \lambda(B) = 1 \) for \( B = V \setminus C_i \), \( i \in \{1, 2\} \), and \( \lambda(B) = 0 \) otherwise.

To show the second inequality, let
\[
\lambda'(B) = \begin{cases} \frac{1}{|A|} & \exists j \in A, B = V \setminus \{j\} \\ \frac{1}{|A|(|A|-1)} & \exists j \in A, B = V \setminus \{j\} \end{cases}
\]
for \( B \subseteq V : B \supseteq A \). Then, \( \lambda' \in \Lambda \) because, for \( i \in V \),
\[
\sum_{B \supseteq A: i \in B} \lambda'(B) = \begin{cases} \frac{1}{|A|} & \{\{V \setminus \{j\} | j \in A \setminus \{i\}\}\} \\ \frac{1}{|A|(|A|-1)} & \{\{A \setminus \{j\} | j \in A \setminus \{i\}\}\} \end{cases}
\]

By (70),
\[
\frac{\alpha(\lambda)}{\lambda} = \min_{\lambda \in \Lambda} \sum_{B \supseteq A: \xi(e) \subseteq B} \lambda'(B)
\]
and so
\[
\alpha(\lambda) = \min_{\lambda \in \Lambda} \left( \frac{A \setminus \{\xi(e)\}}{\lambda} \right) \left( \frac{1}{|A|} + \frac{1}{|A|(|A|-1)} \right)
\]
\[
\geq \frac{|A|-d}{|A|-1}
\]
• Consider the case \( V \setminus A = 0 \). Then,
\[
\{\lambda e \} = |A \setminus \xi(e)|
\]
and so
\[
\alpha(\lambda') = \min_{\lambda \in \Lambda} |A \setminus \{\xi(e)\}| \left( \frac{1}{|A|} + \frac{1}{|A|(|A|-1)} \right)
\]

Thus,
\[
\alpha(\lambda') = \min_{\lambda \in \Lambda} |A \setminus \{\xi(e)\}| \left( \frac{1}{|A|} + \frac{1}{|A|(|A|-1)} \right)
\]

Combining the two cases above, we have
\[
\alpha(\lambda') \geq \begin{cases} \frac{1}{|A|} & d \geq |A|, V \setminus A \neq 0 \\ \frac{1}{|A|} & otherwise. \end{cases}
\]
Hence,
\[
\frac{1}{\min_{\lambda \in \Lambda} \alpha(\lambda)} - 1 \leq \frac{1}{\alpha(\lambda')} - 1 \\
\leq \begin{cases} 
\frac{|A| - 1}{d} & \text{if } d \geq |A|, V \setminus A \neq \emptyset \\
\frac{d - 1}{|A| - 2} & \text{otherwise},
\end{cases}
\]
which can be shown to simplify to the second inequality in (47) as desired. For a complete \(d\)-uniform hypergraph, all the above inequalities can be satisfied with equality, and so equality can also hold for the second inequality in (47).

**ACKNOWLEDGMENT**

The author would like to thank Prof. Navin Kashyap, Praneeth Kumar Vippathalla, and Qiaoqiao Zhao for their valuable comments and discussions.

**REFERENCES**

[1] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography—Part I: Secret sharing,” IEEE Transactions on Information Theory, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[2] U. M. Maurer, “Secret key agreement by public discussion from common information,” IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733–742, 1993.
[3] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” SIAM Journal on Computing, vol. 17, no. 2, pp. 210–229, 1988.
[4] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 344–366, 2000.
[5] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” IEEE Transactions on Information Theory, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
[6] H. Tyagi, “Common information and secret key capacity,” IEEE Transactions on Information Theory, vol. 59, no. 9, pp. 5627–5640, Sep. 2013.
[7] J. Liu, P. Cuff, and S. Verdú, “Secret key generation with limited interaction,” IEEE Transactions on Information Theory, vol. 63, pp. 7358–7381, 2017.
[8] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “Multiterminal secret key agreement at asymptotically zero discussion rate,” in 2018 IEEE International Symposium on Information Theory (ISIT), June 2018, pp. 2654–2658.
[9] C. Chan, M. Mukherjee, P. K. Vippathalla, and Q. Zhou, “Multiterminal secret key agreement with nearly no discussion,” arXiv preprint arXiv:1904.11383, 2019.
[10] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “Upper bounds via lamination on the constrained secrecy capacity of hypergraphical sources,” IEEE Transactions on Information Theory, pp. 1–1, 2019.
[11] S. Nitinawarat and P. Narayan, “Perfect omniscience, perfect secrecy, and Steiner tree packing,” IEEE Transactions on Information Theory, vol. 56, no. 12, pp. 6490–6500, Dec. 2010.
[12] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “Secret key agreement under discussion rate constraints,” in IEEE International Symposium on Information Theory Proceedings (ISIT), June 2017, pp. 1519–1523.
[13] Q. Zhou and C. Chan, “Secrecy capacity under limited discussion rate for minimally connected hypergraphical sources,” CoRR, vol. abs/1805.03110, 2018. [Online]. Available: http://arxiv.org/abs/1805.03110
[14] ———, “Secrecy capacity under limited discussion rate for minimally connected hypergraphical sources,” in 2018 IEEE International Symposium on Information Theory (ISIT). IEEE, 2018, pp. 2664–2668.
[15] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam, “On the public communication needed to achieve sk capacity in the multiterminal source model,” IEEE Transactions on Information Theory, vol. 62, no. 7, pp. 3811–3830, July 2016.
[16] C. Chan, A. Al-Bashabsheh, and Q. Zhou, “Incremental and decremental secret key agreement,” in IEEE International Symposium on Information Theory Proceedings (ISIT), July 2016, pp. 2514–2518.
[17] M. Mukherjee, C. Chan, N. Kashyap, and Q. Zhou, “Bounds on the communication rate needed to achieve sk capacity in the hypergraphical source model,” in IEEE International Symposium on Information Theory Proceedings (ISIT), July 2016, pp. 2504–2508.
[18] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “When is omniscience a rate-optimal strategy for achieving secret key capacity?” in IEEE Information Theory Workshop (ITW), Sep. 2016, pp. 354–358.
[19] ———, “On the optimality of secret key agreement via omniscience,” IEEE Transactions on Information Theory, vol. 64, pp. 2371–2389, 2018.
[20] C. Chan, N. Kashyap, P. K. Vippathalla, and Q. Zhou, “One-shot perfect secret key agreement for finite linear sources,” in 2019 IEEE International Symposium on Information Theory (ISIT), July 2019, pp. 947–951.
[21] C. Chan, “Compressed secret key agreement: maximizing multivariate mutual information per bit,” Entropy, vol. 19, no. 10, 2017.
[22] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik, “Secret key generation for a pairwise independent network model,” IEEE Transactions on Information Theory, vol. 56, no. 12, pp. 6482–6489, Dec 2010.
[23] C. Chan, “Generating secret in a network,” Ph.D. dissertation, Massachusetts Institute of Technology, 2010.
[24] ———, “Linear perfect secret key agreement,” in Information Theory Workshop (ITW), 2011. IEEE, 2011, pp. 723–726.
[25] ———, “Delay of linear perfect secret key agreement,” in Forty-Ninth Annual Allerton Conference on Communication, Control, and Computing, Sep. 2011.
[26] ———, “The hidden flow of information,” in IEEE International Symposium on Information Theory Proceedings (ISIT), Jul. 2011.
[27] ———, “Matroidal undirected network,” in IEEE International Symposium on Information Theory Proceedings (ISIT), July 2012, pp. 1498–1502.
[28] T. A. Courtade and T. R. Halford, “Coded cooperative data exchange for a secret key,” IEEE Transactions on Information Theory, vol. 62, no. 7, pp. 3785–3795, July 2016.
[29] C. Chan and L. Zheng, “Mutual dependence for secret key agreement,” in Proceedings of 44th Annual Conference on Information Sciences and Systems, 2010.
[30] I. Csiszár and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems. Akadémiai Kiadó, Budapest, 1981.
[31] A. Schrijver, Combinatorial Optimization: Polyhedra and Efficiency. Springer, 2002.
[32] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, “On the optimality of secret key agreement via omniscience,” CoRR, vol. abs/1702.07429, 2017. [Online]. Available: http://arxiv.org/abs/1702.07429
[33] I. Csiszár and P. Narayan, “Secrecy capacities for multiterminal channel models,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2437–2452, June 2008.
[34] C. Chan, “On tightness of mutual dependence upperbound for secret-key capacity of multiple terminals,” arXiv preprint arXiv:0805.3209, 2008.
[35] C. Chan, A. Al-Bashabsheh, J. Ebrahimi, T. Kaced, and T. Liu, “Multivariate mutual information inspired by secret-key agreement,” Proceedings of the IEEE, vol. 103, no. 10, pp. 1883–1913, Oct 2015.
[36] C. Chan, A. Al-Bashabsheh, Q. Zhou, T. Kaced, and T. Liu, “Inference clustering: A mathematical theory for data clustering,” IEEE Transactions on Molecular, Biological and Multi-Scale Communications, vol. 2, no. 1, pp. 64–91, June 2016.
[37] C. Chan, A. Al-Bashabsheh, and Q. Zhou, “Change of multivariate mutual information: From local to global,” IEEE Transactions on Information Theory, vol. PP, no. 99, pp. 1–1, 2017.
[38] C. Chan, K. W. Shum, and Q. T. Sun, “Combinatorial flow over cyclic linear networks,” in IEEE Information Theory Workshop (ITW), Sep. 2013, pp. 1–5.
[39] C. Chan, “Cyclic linking network,” in IEEE International Symposium on Information Theory Proceedings (ISIT), July 2013, pp. 789–793.
[40] I. Csiszar and J. Korner, Information Theory: Coding Theorems for Discrete Memoryless Systems, 2nd ed. Cambridge University Press, 2011.
[41] S. Fujishige, “Polymatroidal dependence structure of a set of random variables,” Information and Control, vol. 39, no. 1, pp. 55 – 72, 1978.
[42] ———, Submodular functions and optimization, 2nd ed. Elsevier, 2005.