Secret Key Capacity: Talk or Keep Silent?

Huishuai Zhang
Dept. of EECS
Syracuse University
Syracuse, NY 13244
Email: hzhan23@syr.edu

Yingbin Liang
Dept. of EECS
Syracuse University
Syracuse, NY 13244
Email:yliang06@syr.edu

Lifeng Lai
Dept of ECE
Worcester Polytechnic Institute
Worcester, MA 01609
Email: llai@wpi.edu

***Abstract*—The problem of when all terminals must talk to achieve the secrecy capacity in the multiterminal source model is investigated. Two conditions under which respectively a given terminal does not need to and must talk to achieve the secrecy capacity are characterized. The cases when all terminals must talk to achieve secrecy capacity are shown to be many more than those conjectured in [1] for systems with four or more terminals. There is a gap between the above two conditions, in which whether a given terminal need to talk is not clear. A conjecture is further made in order to narrow down the gap.**

***Keywords*—Mutual dependence, omniscience scheme, secret key capacity, source model**

I. Introduction

Consider the secret key generation problem among m terminals, in which each terminal observes one component of a correlated vector source and all of the m terminals wish to agree on a common secret key (SK) via public discussion. The SK capacity, which is the maximum achievable key rate, is established in [2] by using the "omniscience" scheme. Namely, each terminal reveals information to public until the omniscience attains, i.e., every terminal knows all terminals' observations. However, such an omniscience scheme is not always necessary to achieve the SK capacity. In fact, it is pointed out in [2, Sec. VI] that neither transmissions by all the terminals nor omniscience at all terminals is necessary for achieving the SK capacity. This can be easily seen in the two-terminal scenario [3], [4], where one way communication is sufficient to achieve the SK capacity. Even for the case with $m > 2$, [2] provides an example, in which not all terminals need to talk to achieve the SK capacity.

More recently, [1] formally studied the problem to address when all terminals must talk to achieve the SK capacity. A sufficient condition is established , under which all terminals must talk to achieve the SK capacity. Such a sufficient condition was also shown to be necessary when $m = 3$. It was further conjectured that the above sufficient condition is also necessary in general for the case with $m > 3$.

When $m > 3$, it is in general very difficult to verify the necessary condition that requires all terminals to talk to achieve the SK capacity. As pointed out in the previous work [5], the problem complexity is related to the expression of the SK capacity for multiple terminals, which equals to the mutual dependence as shown in [6]. The mutual dependence as an extension of the mutual information among more than two variables, is defined to be minimization over all partitions of source components (i.e., terminals in the system). The number of feasible partitions increases exponentially with the number of terminals. For instance, there are four feasible partitions for a three-terminal system, but fourteen partitions for a four-terminal system. The proof of the necessary condition for the case with $m = 3$ in [1], explored the mutual dependence of three sources based on explicit analysis of the four partitions. However, when m becomes large, such an approach may not be tractable.

In this paper, we establish a critical lemma that significantly simplifies the expression of the SK capacity when muting a specific terminal, which enables the analysis when $m > 3$. Specifically, we address the problem of when all terminals must talk from two directions. We first establish a sufficient condition under which a specific terminal does not need to talk to achieve the SK capacity. We then provide a sufficient condition under which a specific terminal must talk. Our results suggest that there are many more cases when all terminals must talk than those conjectured in [1] when $m > 3$. We also analyze the gap between the two conditions and provide further result narrowing down the gap.

The paper is organized as follows. Section II introduces model, notations and some previous results. Section III provides our main theorems on characterizing the conditions under which a terminal does not need to and must talk to achieve the SK capacity, respectively. Section IV outlines the proofs of the main theorems. Section V concludes this paper with discussion.

II. Model, Notations and Preliminaries

We describe the model of interest, and provide some results developed for this model in existing literature that are useful for establishing our results here.

Suppose m terminals observe outputs of a discrete memoryless vector source $(X_1, ..., X_m)$ with each terminal observing one component. More specifically, terminal i observes n i.i.d repetitions of X_i denoted as X_i^n for $i = 1, 2, \ldots, m$. All m terminals wish to agree on a secret key. Each terminal can reveal any causal information, i.e., a deterministic function of the information available to that terminal at the time, to public, and all other terminals including the eavesdropper can receive the information without ambiguity. The public discussion can be interactive and up to r rounds.

For clear understanding, we explain some notations here, which will be used throughout the paper. We use numbers such as 1, 2 and lower letters u and m to denote terminals. We use calligraphic letters $\mathcal{M}, \mathcal{T}$ or numbers with square bracket $[m]$

to denote a set of terminals, i.e., $[m] = \{1, 2, ..., m\}$, and consequently $X_{\mathcal{M}} = (X_i, i \in \mathcal{M})$ and $X_{[m]} = (X_j, j = 1, 2, \ldots, m)$ denote the same random vector. The subset relation symbol "$\subset$" means proper subset, i.e., $\mathcal{T} \subset \mathcal{M}$ indicates $\mathcal{T} \neq \mathcal{M}$. Furthermore, $C(\mathcal{M})$ denotes the SK capacity without any extra assumption on public discussion and $C(\mathcal{M}\|\mathcal{T})$ denotes the SK capacity when only the terminals in $\mathcal{T}$ are allowed to talk over the public channel.

The SK capacity $C(\mathcal{M})$ for the above model was established in [2] as we describe below.

Theorem 1. *([2, Theorem 1]) The SK capacity $C(\mathcal{M})$ for a set $\mathcal{M}$ of terminals equals*

$$C(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{CO}, \tag{1}$$

where R_{CO} is the minimum communication rate to achieve omniscience and equals

$$R_{CO} = \min_{R_{\mathcal{M}} \in \mathcal{R}(\mathcal{M})} \sum_{i \in \mathcal{M}} R_i, \tag{2}$$

and

$$\mathcal{R}(\mathcal{M}) = \left\{ R_{\mathcal{M}} : \sum_{i \in \mathcal{B}} R_i \geq H(X_{\mathcal{B}} | X_{\mathcal{B}^c}), \forall \mathcal{B} \subset \mathcal{M}, \mathcal{B} \neq \emptyset \right\}. \tag{3}$$

One interpretation of the SK capacity in (1) is clear from its expression, as subtracting from the entire source information $H(X_{\mathcal{M}})$ the minimum transmission rate R_{CO} to achieve omniscience at all terminals. In fact, there is an alternative interpretation of the SK capacity. In the two-terminal case where $\mathcal{M} = [2]$, $C(\mathcal{M})$ is given by the mutual information $I(X_1; X_2)$ between two sources X_1 and X_2. Such interpretation of the SK capacity is generalized to the case with $m > 2$ in [6], [7] by introducing a notion of *mutual dependence*, which can be viewed as an extension of mutual information to more than two variables.

Definition 1. *(Mutual Dependence [6]) For any finite-value random vector $X_{\mathcal{M}} := (X_i : i \in \mathcal{M})$ with $|\mathcal{M}| \geq 2$, the mutual dependence of $X_{\mathcal{M}}$ is defined as*

$$I(X_{\mathcal{M}}) := \min_{\mathscr{P} \in \Pi} \frac{1}{|\mathscr{P}| - 1} D\left(P_{X_{\mathcal{M}}} \| \prod_{\mathcal{T} \in \mathscr{P}} P_{X_{\mathcal{T}}} \right), \tag{4}$$

where $\mathscr{P}$ is one partition of $\mathcal{M}$ into at least 2 non-empty sets, Π is the collection of all such partitions $\mathscr{P}$, and $D(p\|q)$ is the KL divergence between the distributions p and q.

The expression (4) can be intuitively understood as the minimum distance between the joint distribution of the source and the product of marginal distributions of partitioned sets over all feasible partitions. It measures the statistical correlation among the sets in a partition of $\mathcal{M}$.

Example 1. *If $\mathcal{M} := [2] := \{1, 2\}$, then the mutual dependence reduces to the mutual information, i.e.,*

$$I(X_{[2]}) = I(X_1; X_2).$$

If $\mathcal{M} = [3]$, then the mutual dependence is given by

$$I(X_{[3]}) = \min \Big\{ I(X_1; X_2 X_3), I(X_2; X_1 X_3), I(X_3; X_1 X_2), \frac{1}{2} \left(\sum_{i=1}^{3} H(X_i) - H(X_1 X_2 X_3) \right) \Big\}.$$

It was shown in [6], [7] that if all terminals are required to agree on a secret key, then the SK capacity (1) equals to the mutual dependence (4).

Theorem 2. *([6], [7]) Given a finite set $\mathcal{M}$ with $|\mathcal{M}| \geq 2$, the mutual dependence in* (4) *satisfies*

$$I(X_{\mathcal{M}}) = C(\mathcal{M}). \tag{5}$$

The SK capacity in Theorem 1 and 2 is with respect to when all terminals are allowed to talk during public discussion. In [8], the SK capacity is established when only a subset of terminals are allowed to talk publicly, which is stated as the following theorem.

Theorem 3. *([8, Theorem 6]) Consider a multiterminal source model. All m terminals are required to agree on a key but only the first u terminals can talk publicly. Then the SK capacity is given by*

$$C([m] \| [u]) = H(X_{[u]}) - \min_{(R_1, R_2, \ldots, R_u) \in \mathcal{R}} \left(\sum_{i=1}^{u} R_i \right), \tag{6}$$

where

$$\mathcal{R} = \big\{ (R_1, \ldots, R_u) : \sum_{j \in \mathcal{B} \cap [u]} R_j \geq H(X_{\mathcal{B} \cap [u]} | X_{\mathcal{B}^c}), \forall \mathcal{B} \subset [m], \mathcal{B} \cap [u] \neq \emptyset \big\}.$$

In general, it is not easy to compare (6) with (1) directly. It is then desirable to develop an equivalent form for (6) based on the mutual dependence so that comparison between such a form and (4) can be easily done, which provides comparison between (6) and (1). One major step in our analysis in this paper lies in the establishment of an equivalent form for (6) when one terminal is muted.

III. Main Results

We first introduce a lemma, which play a critical role in the proof of the main results.

Lemma 1. *Given a finite set $\mathcal{M}$ with $|\mathcal{M}| = m \geq 2$. For any $u \in \mathcal{M}$ and $\mathcal{T} = \mathcal{M} \setminus u$, we have*

$$C(\mathcal{M} \| \mathcal{T}) = \min\{ I(X_u; X_{\mathcal{T}}), I(X_{\mathcal{T}}) \}.$$

Lemma 1 is useful for proving our main results in Theorems 4 and 5. It considers a special case of Theorem 3 when only one terminal (i.e., terminal u) is muted. This lemma establishes the SK capacity for this case in a form of mutual dependence, which can be more conveniently compared with the SK capacity when all terminals are allowed to talk publicly.The proof of Lemma 1 is presented in Sec. IV.

In the following theorem, we characterize a condition under which a terminal is not necessary to talk to achieve the SK capacity.

TABLE I. SHOULD TERMINAL u TALK OR KEEP SILENT?

$I(X_u;X_{\mathcal{T}})=C(\mathcal{M})$	$I(X_u;X_{\mathcal{T}})>C(\mathcal{M})$			
	$\exists\ v\ \ s.t.$ $X_u-X_v-X_{\mathcal{M}\setminus\{u,v\}}$	$\mathscr{P}_2$ *minimizes* $I(X_{\mathcal{M}})$ *and* $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ *with* $\lvert\mathcal{T}_1\rvert>1$	$\mathscr{P}_2$ *minimizes* $I(X_{\mathcal{M}})$ *and* $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ *does not hold*	$\mathscr{P}_1$ minimizes $I(X_{\mathcal{M}})$
Need not talk		Not clear	Must talk	

Theorem 4. *Suppose a set $\mathcal{M}$ of terminals wish to agree on a secret key via public discussion. Given a single terminal u and $\mathcal{T}=\mathcal{M}\setminus\{u\}$, if partition $\mathscr{P}: X_u|X_{\mathcal{T}}$ is a minimizer of the mutual dependence $I(X_{\mathcal{M}})$ defined as* (4) *(and hence $I(X_{\mathcal{M}})=I(X_u;X_{\mathcal{T}})$), then there exists a scheme that achieves the SK capacity with terminal u being silent.*

Intuitively, the fact that $\mathscr{P}: X_u|X_{\mathcal{T}}$ is a minimizer of the mutual dependence $I(X_{\mathcal{M}})$ implies that the least correlation among terminals is between X_u and $X_{\mathcal{T}}$. Thus, one natural scheme with u being silent is to let the terminals in the set $\mathcal{T}$ first attain omniscience of $X_{\mathcal{T}}^n$, and then key generation reduces to the problem between two terminals u and $\mathcal{T}$. Thus, only terminals in $\mathcal{T}$ talking is sufficient to achieve the SK capacity. The proof of Theorem 4 is presented in Sec. IV.

Theorem 4 shows that if $I(X_{\mathcal{M}})=I(X_u;X_{\mathcal{T}})$, then terminal u does not need to talk to achieve the SK capacity. It is then interesting to ask if the condition is not satisfied, does terminal u need to talk to achieve the SK capacity? The following theorem answers this question with an additional assumption. The proof of Theorem 5 is presented in Sec. IV.

Theorem 5. *Consider a given terminal u and $\mathcal{T}=\mathcal{M}\setminus\{u\}$ with $I(X_u;X_{\mathcal{T}})>I(X_{\mathcal{M}})$. If (i) partition $\mathscr{P}_1: X_u\big|X_{\mathcal{T}_1}\big|\dots\big|X_{\mathcal{T}_k}$ is a minimizer of $I(X_{\mathcal{M}})$, or if (ii) partition $\mathscr{P}_2: X_uX_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_k}$ is a minimizer of $I(X_{\mathcal{M}})$ and $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ does not hold, where $k>1$ and $\mathcal{T}_i\neq\emptyset$ for all $i\in[k]$, then terminal u must talk in order to achieve the SK capacity.*

Remark 1. *If multiple terminals satisfy the assumptions in the above theorem, then they all must talk to achieve the SK capacity.*

In fact, [1] has shown that a sufficient condition under which all terminals must talk is that the singleton partition $\mathscr{P}_S: X_1\big|X_2\big|\dots\big|X_m$ is the unique minimizer of $I(X_{\mathcal{M}})$. Furthermore, [1] has conjectured that this sufficient condition is also necessary, which suggests that only in the case where the singleton partition is the unique minimizer of $I(X_{\mathcal{M}})$ all terminals must talk.

Theorem 5 indicates the conjecture that the singleton partition uniquely minimizing $I(X_{\mathcal{M}})$ is the only case in which all terminals must talk is not complete. It is clear that condition (i) includes singleton partition case. Hence, in addition to the singleton partition case as conjectured in [1], condition (ii) suggests that there are many more cases characterized by non-singleton cases under which all terminals must talk.

Example 2. *For $\mathcal{M}=[3]$, if $I(X_1;X_2X_3)$ minimizes $I(X_{[3]})$, then Theorem 4 suggests that X_1 does not need to talk to achieve the SK capacity. Furthermore, if $1/2\big[\sum_{i=1}^3 H(X_i)-H(X_1X_2X_3)\big]$ is the unique minimizer of $I(X_{[3]})$, then in order to achieve the SK capacity Theorem 5 suggests that all terminals must talk. These conclusions coincide with the results in [1] for the case with three terminals.*

Theorem 4 shows that if $I(X_u;X_{\mathcal{T}})=I(X_{\mathcal{M}})$ then terminal u does not need to talk to achieve the SK capacity. On the other hand, Theorem 5 shows that if $I(X_u;X_{\mathcal{T}})>I(X_{\mathcal{M}})$ and under either condition (i) or (ii), then terminal u must talk. The gap between the two conditions corresponds to only the case where partition $\mathscr{P}_2$ is a minimizer of $I(X_{\mathcal{M}})$ and the Markov chain $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ holds. For such a case, Theorem 4 and 5 do not provide a conclusive answer about whether terminal u must talk or not. In the next theorem, we provide further understanding of one sub case. The proof is presented in Sec. IV.

Theorem 6. *Given a single terminal u, if there exists another distinct terminal v such that $X_u-X_v-X_{\mathcal{M}\setminus\{u,v\}}$ holds, then there exists a scheme that achieves the SK capacity with terminal u being silent.*

The above theorem suggests that if there is a single terminal v that can represent u, i.e., $X_u-X_v-X_{\mathcal{M}\setminus\{u,v\}}$ holds, then terminal u does not need to talk to achieve the SK capacity. Intuitively, we can view v as a proxy of u in the key agreement process: let v first agree on a key with terminals in $\mathcal{M}\setminus\{u,v\}$ and then let v share such a key with u.

In Table I, we summarize our results in Theorem 4-6. It can be seen that the problem is still open for the scenario in which $\mathscr{P}_2$ minimizes $I(X_{\mathcal{M}})$ and $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ holds with $|\mathcal{T}_1|\geq 2$. For this scenario, we make the following conjecture based on our understanding of the problem.

Conjecture 1. *If partition $\mathscr{P}: X_uX_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_k}$ minimizes $I(X_{\mathcal{M}})$ and $X_u-X_{\mathcal{T}_1}-X_{\mathcal{T}\setminus\mathcal{T}_1}$ holds with $|\mathcal{T}_1|\geq 2$, and if $I(X_u;X_{\mathcal{T}_1})=I(X_{\{u\}\cup\mathcal{T}_1})$, then terminal u does not need to talk to achieve the SK capacity.*

IV. TECHNICAL PROOFS

Proof of Lemma 1. Applying Theorem 3, we have

$$C(\mathcal{M}\big\|\mathcal{T})=H(X_{\mathcal{T}})-\min_{(R_j,j\in\mathcal{T})\in\mathcal{R}}\left(\sum_{j\in\mathcal{T}}R_j\right)$$

where

$$\mathcal{R}=\big\{(R_j:j\in\mathcal{T}):\sum_{j\in\mathcal{B}\cap\mathcal{T}}R_j\geq H(X_{\mathcal{B}\cap\mathcal{T}}|X_{\mathcal{B}^c}),\ \forall\mathcal{B}\subset\mathcal{M},\mathcal{B}\cap\mathcal{T}\neq\emptyset\big\}$$

Hence, all the rate tuples $(R_j:j\in\mathcal{T})\in\mathcal{R}$ satisfy the following constraints.

(1) If $\mathcal{B}\subset\mathcal{T}$, then

$$\sum_{j\in\mathcal{B}} R_j \geq H(X_{\mathcal{B}}|X_{\mathcal{B}^c}) = H(X_{\mathcal{B}}|X_{\mathcal{B}^{c'}}X_u),$$

where the complement operation c is with respect to the whole set $\mathcal{M}$ and c' is with respect to the set $\mathcal{T}$.

(2) If $\mathcal{B}=\mathcal{T}$, then $\sum_{j\in\mathcal{T}} R_j \geq H(X_{\mathcal{T}}|X_u)$.

(3) If $\mathcal{B}\ni u$, then let $\mathcal{B}=\tilde{\mathcal{B}}\cup\{u\}$, and consequently $\tilde{\mathcal{B}}\subset\mathcal{T}$ and $\tilde{\mathcal{B}}\neq\emptyset$. We have

$$\sum_{j\in\mathcal{B}\cap\mathcal{T}} R_j = \sum_{j\in\tilde{\mathcal{B}}} R_j \geq H(X_{\mathcal{B}\cap\mathcal{T}}|X_{\mathcal{B}^c}) = H(X_{\tilde{\mathcal{B}}}|X_{\tilde{\mathcal{B}}^{c'}})$$

Combining the above three cases, we conclude that the following conditions equivalently characterize the region $\mathcal{R}$:

$$\sum_{j\in\mathcal{T}} R_j \geq H(X_{\mathcal{T}}|X_u), \tag{7}$$

$$\sum_{j\in\mathcal{B}} R_j \geq H(X_{\mathcal{B}}|X_{\mathcal{B}^{c'}}), \quad \forall\mathcal{B}\subset\mathcal{T}, \mathcal{B}\neq\emptyset. \tag{8}$$

Next we consider another region $\mathcal{R}'$ which consists of rate tuples $(R_j : j\in\mathcal{T})$ with which the terminals in $\mathcal{T}$ can establish the omniscience of $X_{\mathcal{T}}^n$. Hence, using Theorem 1, we obtain

$$\mathcal{R}' = \big\{(R_j : j\in\mathcal{T}) : \sum_{j\in\mathcal{B}} R_j \geq H(X_{\mathcal{B}}|X_{\mathcal{B}^{c'}}), \\ \forall\mathcal{B}\subset\mathcal{T}, \mathcal{B}\neq\emptyset\big\}.$$

It is clear that if all rate tuples $(R_j : j\in\mathcal{T})\in\mathcal{R}'$ satisfy

$$\sum_{j\in\mathcal{T}} R_j \geq H(X_{\mathcal{T}}|X_u),$$

then $\mathcal{R}=\mathcal{R}'$, and consequently $C(\mathcal{M}\big\|\mathcal{T}) = C(\mathcal{T})$. Otherwise if

$$\min_{(R_j:j\in\mathcal{T})\in\mathcal{R}'} \left(\sum_{j\in\mathcal{T}} R_j\right) < H(X_{\mathcal{T}}|X_u),$$

then because of the convexity of the set $\mathcal{R}'$, there must exist a tuple $(R_j : j\in\mathcal{T})\in\mathcal{R}'$ with $\sum_{j\in\mathcal{T}} R_j = H(X_{\mathcal{T}}|X_u)$, which implies the following

$$\min_{(R_j:j\in\mathcal{T})\in\mathcal{R}} \left(\sum_{j\in\mathcal{T}} R_j\right) = H(X_{\mathcal{T}}|X_u),$$

and consequently, $C(\mathcal{M}\|\mathcal{T}) = I(X_u;X_{\mathcal{T}})$. Thus, we conclude

$$C(\mathcal{M}\big\|\mathcal{T}) = \min\left\{I(X_u;X_{\mathcal{T}}), C(\mathcal{T})\right\}.$$

Proof of Theorem 4. It is sufficient to show that $C(\mathcal{M}) = C(\mathcal{M}\big\|\mathcal{T})$. Due to the assumption of the theorem $I(X_u;X_{\mathcal{T}}) = C(\mathcal{M})$ and Lemma 1 $C(\mathcal{M}\|\mathcal{T}) = \min\{I(X_u;X_{\mathcal{T}}), I(X_{\mathcal{T}})\}$, it is then sufficient to show that $I(X_u;X_{\mathcal{T}}) \leq I(X_{\mathcal{T}})$.

Suppose that a partition

$$\mathscr{P} : X_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_{|\mathscr{P}|}}, \ \ where \ \bigcup_{\mathcal{T}_i\in\mathscr{P}} \mathcal{T}_i = \mathcal{T}$$

minimizes $I(X_{\mathcal{T}})$. Then,

$$I(X_{\mathcal{T}}) = \frac{1}{|\mathscr{P}|-1}\left(\sum_{\mathcal{T}_i\in\mathscr{P}} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{T}})\right). \tag{9}$$

Consider another partition

$$\mathscr{P}' : X_u\big|X_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_{|\mathscr{P}|}},$$

then $\mathscr{P}'\in\Pi_{\mathcal{M}}$ by definition. Thus we have

$$\begin{aligned} I(X_u;X_{\mathcal{T}}) &= C(\mathcal{M}) \\ &\leq \frac{1}{|\mathscr{P}'|-1}\left(H(X_u) + \sum_{\mathcal{T}_i\in\mathscr{P}} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right) \\ &= \frac{|\mathscr{P}|-1}{|\mathscr{P}|} I(X_{\mathcal{T}}) + \frac{1}{|\mathscr{P}|} I(X_u;X_{\mathcal{T}}), \end{aligned}$$

which implies that $I(X_u;X_{\mathcal{T}}) \leq I(X_{\mathcal{T}})$.

Proof of Theorem 5. We first show that condition (i) implies that terminal u must talk. It is sufficient to show that $C(\mathcal{M}\big\|\mathcal{T}) < C(\mathcal{M})$. Since $I(X_u;X_{\mathcal{T}}) > I(X_{\mathcal{M}})$ and $C(\mathcal{M}) \geq C(\mathcal{M}\big\|\mathcal{T}) = \min\{I(X_u;X_{\mathcal{T}}), I(X_{\mathcal{T}})\}$, it is sufficient to show that $I(X_{\mathcal{M}}) > I(X_{\mathcal{T}})$. Towards this end, we derive

$$\begin{aligned} I(X_{\mathcal{M}}) &= \frac{1}{|\mathscr{P}_1|-1}\left(H(X_u) + \sum_{i=1}^{|\mathscr{P}_1|-1} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right) \\ &\geq \frac{|\mathscr{P}_1|-2}{|\mathscr{P}_1|-1} I(X_{\mathcal{T}}) + \frac{1}{|\mathscr{P}_1|-1} I(X_u;X_{\mathcal{T}}). \end{aligned}$$

Rearranging the terms and using the fact $I(X_u;X_{\mathcal{T}}) > I(X_{\mathcal{M}})$, we obtain $I(X_{\mathcal{M}}) > I(X_{\mathcal{T}})$.

We next show that condition (ii) implies that terminal u must talk. We derive

$$\begin{aligned} I(X_{\mathcal{M}}) &= \frac{1}{|\mathscr{P}_2|-1}\left(H(X_u|X_{\mathcal{T}_1}) + \sum_{i=1}^{|\mathscr{P}_2|} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right) \\ &\geq I(X_{\mathcal{T}}) + \frac{1}{|\mathscr{P}_2|-1}\left(H(X_u|X_{\mathcal{T}_1}) - H(X_u|X_{\mathcal{T}})\right) \\ &> I(X_{\mathcal{T}}), \end{aligned}$$

where the last step is because $X_u - X_{\mathcal{T}_1} - X_{\mathcal{T}\setminus\mathcal{T}_1}$ does not hold by assumption. This concludes the proof.

Proof of Theorem 6. We first show that if $X_u - X_v - X_{\mathcal{M}\setminus\{u,v\}}$ holds, then there must exist a partition $\mathscr{P}$ containing X_u and X_v in the same set that minimizes $I(X_{\mathcal{M}})$.

It is sufficient to show that if a partition with the form $\mathscr{P}' : X_uX_{\mathcal{T}_1}\big|X_vX_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_k}$ minimizes $I(X_{\mathcal{M}})$, then there always exists another partition $\mathscr{P} : X_uX_vX_{\mathcal{T}_2}\big|X_{\mathcal{T}_1}\big|\dots\big|X_{\mathcal{T}_k}$ which yields no greater value of the objective function of (4).

Case 1: $\mathcal{T}_1\neq\emptyset$. It implies that $|\mathscr{P}'| = |\mathscr{P}| = k$. It is sufficient to show

$$\begin{aligned} &\frac{1}{|\mathscr{P}'|-1}\left(H(X_uX_{\mathcal{T}_1}) + H(X_vX_{\mathcal{T}_2}) + \sum_{i=3}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right) \\ &\geq \frac{1}{|\mathscr{P}|-1}\left(H(X_uX_vX_{\mathcal{T}_2}) + \sum_{i=1,3}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right), \end{aligned}$$

which can be shown equivalent to

$$H(X_u|X_{\mathcal{T}_1}) \geq H(X_u|X_v).$$

Case 2: $\mathcal{T}_1 = \emptyset$. In this case, $|\mathscr{P}'| = k$ and $|\mathscr{P}| = k-1$. We want to show

$$\frac{1}{|\mathscr{P}'|-1}\left(H(X_u) + H(X_vX_{\mathcal{T}_2}) + \sum_{i=3}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right)$$
$$\geq \frac{1}{|\mathscr{P}|-1}\left(H(X_uX_vX_{\mathcal{T}_2}) + \sum_{i=3}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right),$$

which can be shown equivalent to

$$I(X_u; X_{\mathcal{T}}) \geq I(X_{\mathcal{M}}).$$

Thus, without loss of generality, we suppose that partition $\mathscr{P}$ with the form $X_uX_vX_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_k}$ minimizes $I(X_{\mathcal{M}})$. Furthermore, we already know that if $I(X_u; X_{\mathcal{T}}) = I(X_{\mathcal{M}})$, then terminal u does not need to talk to achieve the SK capacity. Thus without loss of generality, we assume that $I(X_u; X_{\mathcal{T}}) > I(X_{\mathcal{M}})$ strictly in the following proof.

Using Lemma 1, we obtain

$$I(X_u; X_{\mathcal{T}}) > C(\mathcal{M}) \geq C(\mathcal{M}\big\|\mathcal{T}) = \min\{I(X_u; X_{\mathcal{T}}), I(X_{\mathcal{T}})\}.$$

Hence, $C(\mathcal{M}\big\|\mathcal{T}) = I(X_{\mathcal{T}})$. It is then sufficient to show that $I(X_{\mathcal{T}}) = I(X_{\mathcal{M}})$. We derive

$$\begin{aligned} I(X_{\mathcal{M}}) &= \frac{1}{|\mathscr{P}|-1}\left(H(X_uX_vX_{\mathcal{T}_1}) + \sum_{i=2}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right) \\ &= \frac{1}{|\mathscr{P}|-1}\left(H(X_vX_{\mathcal{T}_1}) + \sum_{i=2}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{T}})\right) \\ &\geq I(X_{\mathcal{T}}). \end{aligned}$$

The above equality holds if the partition $\mathscr{P}_{\mathcal{T}}$: $X_vX_{\mathcal{T}_1}\big|X_{\mathcal{T}_2}\big|\dots\big|X_{\mathcal{T}_k}$ minimizes $C(\mathcal{T})$. We note that $|\mathscr{P}_{\mathcal{T}}| = |\mathscr{P}| = k$. It is sufficient to show that for any partition $\mathscr{P}'_{\mathcal{T}} : X_{\mathcal{D}_1}\big|X_{\mathcal{D}_2}\big|\dots\big|X_{\mathcal{D}_l}$ such that $\bigcup_{i=1}^{l}\mathcal{D}_i = \mathcal{T}$, we have

$$\frac{1}{|\mathscr{P}_{\mathcal{T}}|-1}\left(H(X_vX_{\mathcal{T}_1}) + \sum_{i=2}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{T}})\right)$$
$$\leq \frac{1}{|\mathscr{P}'_{\mathcal{T}}|-1}\left(\sum_{j=1}^{l} H(X_{\mathcal{D}_j}) - H(X_{\mathcal{T}})\right). \tag{10}$$

Without loss of generality, we assume $v \in \mathcal{D}_1$. Then that (10) holds is equivalent to

$$\frac{1}{|\mathscr{P}|-1}\left(H(X_uX_vX_{\mathcal{T}_1}) + \sum_{i=2}^{k} H(X_{\mathcal{T}_i}) - H(X_{\mathcal{M}})\right)$$
$$\leq \frac{1}{|\mathscr{P}'_{\mathcal{T}}|-1}\left(H(X_uX_{\mathcal{D}_1}) + \sum_{j=2}^{l} H(X_{\mathcal{D}_j}) - H(X_{\mathcal{M}})\right) \tag{11}$$

because $H(X_u|X_vX_{\mathcal{T}_1}) - H(X_{\mathcal{T}}) = 0$ and $H(X_u|X_{\mathcal{D}_1}) - H(X_u|X_{\mathcal{T}}) = 0$ by the Markov chain assumption. In fact, (11) holds because partition $\mathscr{P}$ is a minimizer of $I(X_{\mathcal{M}})$.

Thus, $I(X_{\mathcal{T}}) = I(X_{\mathcal{M}})$, and terminal u does not need to talk to achieve the SK capacity.

V. Discussion and Conclusion

In this paper, we studied the problem of when all terminals must talk to achieve the SK capacity in the multi-terminal source model, originally proposed in [1]. We characterized the sufficient conditions under which a terminal does not need to talk and must talk to achieve the SK capacity. Our results confirmed the result of [1] when $m = 3$ and characterized more cases under which all terminals must talk than those conjectured in [1] when $m > 3$.

A closely related problem is to characterize the minimum sum rate in public discussion to achieve the SK capacity for the source-type model. [9] studied the two-terminal case and showed that the minimum transmission rate equals interactive CI minus the SK capacity, where the interactive CI is defined as a quantity related to and no less than Wyner's common information [10]. This characterization provides the theoretical minimum interactive transmission rate to establish the SK capacity. Furthermore, if we confine ourself within non-interactive transmission, the Slepian-Wolf source coding plays a pivotal role. Then it is also interesting to understand the minimum non-interactive transmission rate for achieving the SK capacity. We have strong belief that there is close connection between this question and the problem studied here and in [1].

Acknowledgment

The work of H. Zhang and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grant CNS-11-16932. The work of L. Lai was supported by a National Science Foundation CAREER Award under Grant CCF-13-18980 and by the National Science Foundation under Grant CNS-13-21223.

References

[1] M. Mukherjee, N. Kashyap, and Y. Sankarasubramaniam. Achieving sk capacity in the source model: When must all terminals talk? In *Proc. IEEE Int. Symp. Information Theory (ISIT)*, pages 1156–1160, Honolulu, HI, USA, June 2014.

[2] I. Csiszár and P. Narayan. Secrecy capacities for mulitple terminals. *IEEE Trans. Inform. Theory*, 50(12):3047–3061, December 2004.

[3] U. M. Maurer. Secrete key agreement by public discussion based on common information. *IEEE Trans. Inform. Theory*, 39(5):733–742, May 1993.

[4] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography-Part I: Secret sharing. *IEEE Trans. Inform. Theory*, 39(4):1121–1132, July 1993.

[5] H. Zhang, Y. Liang, and L. Lai. Helper-assisted asymmetric two key generation. In *Proc. Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, USA, November 2014.

[6] C. Chan and L. Zheng. Mutual dependence for secret key agreement. In *Proc. Conf. on Information Sciences and Systems (CISS)*, Princeton University, NJ, USA, March 2010.

[7] C. Chan. Generating secret in a network. Ph.D. dissertation, Massachusetts Institute of Technology, 2010.

[8] A.A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminals -part i. *IEEE Trans. Inform. Theory*, 56(8):3973–3996, Aug 2010.

[9] H. Tyagi. Common information and secret key capacity. *IEEE Trans. Inform. Theory*, 59(9):5627–5640, Septempber 2013.

[10] A.D. Wyner. The common information of two dependent random variables. *IEEE Trans. Inform. Theory*, 21(2):163–179, Mar 1975.