Secret Key Agreement under Discussion Rate Constraints

Chung Chan, Manuj Mukherjee, Navin Kashyap and Qiaoqiao Zhou

***Abstract*—For the multiterminal secret key agreement problem, new single-letter lower bounds are obtained on the minimum public discussion rate required to achieve any given secret key rate below the secrecy capacity. The results apply to the general source model without helpers or wiretapper's side information, but can be strengthened for hypergraphical sources. In particular, for the pairwise independent network, our results yield a complete characterization of the maximum secret key rate achievable under a constraint on the total discussion rate.**

I. Introduction

We consider the multiterminal secret key agreement by public discussion introduced by Csiszár and Narayan [2], under the source model without helpers or wiretapper's side information. The maximum achievable secret key rate with unlimited public discussion, called the secrecy capacity, was determined in [2], the argument for achievability using a key generation protocol in which all terminals attained omniscience of the source. However, it was also pointed out there that the public discussion rate in the omniscience scheme need not, in general, be the minimum required for achieving the secrecy capacity. The determination of the minimum rate of public discussion, which we refer to as the *communication complexity*, was left as an open problem.

For the 2-user case, Tyagi [3] derived a multi-letter characterization of the communication complexity, which involved an asymptotic version of the Wyner common information. These ideas were extended in [4] to the multiterminal setting, where a lower bound was given for the communication complexity in terms of a multiterminal Wyner common information defined using the notion of multivariate mutual information (MMI) [5]. For the special case of a pairwise independent network (PIN) [6], the bound leads to a single-letter necessary and sufficient condition for the omniscience strategy in [2] to achieve the communication complexity. The general multiterminal lower bound of [4] was simplified to an easily computable single-letter bound in [7]. Also in that work, the condition for the optimality of omniscience was generalized from PINs to hypergraphical sources (as defined in [8]), using the idea of decremental secret key agreement [9], an idea that had already been used in [10] to derive upper bounds. Unfortunately, the single-letter lower bound of [7] can be loose even for simple PINs, and it was conjectured there that the lower bound was not good enough to yield a condition for the optimality of omniscience for general sources.

In resolving the above conjecture, we discovered new techniques that can improve the lower bound further. Although these techniques are also based on the idea of MMI, they work quite differently from the idea of Wyner common information in [3, 4]. We apply these techniques to obtain an outer bound on the region of achievable secret key rate and discussion rate tuples. In particular, for PIN models on trees our outer bound turns out to be an exact characterization. In contrast with the rate region characterized in [11] for two terminals using the idea of two-way interactive source coding [12], the result is the first instance of an exact and easily computable characterization for the case with at least three terminals with unlimited number of rounds of interactive discussion. We also use the outer bound to characterize the communication complexity, and more generally, the maximum secret key rate achievable under any given total discussion rate, referred to as the *rate-constrained secrecy capacity*.

The remainder of this paper is organized as follows. After motivating the problem with an example in Section II, we give a mathematical formulation of the problem in Section III. Our main results are presented in Section IV, with sketches of some of the proofs; complete proofs of all the results can be found in the full version of this paper [1]. We conclude in Section V with some open problems.

II. Motivation

We first motivate the idea of secret key agreement and the main results informally using a simple example. Let $\mathsf{X}_{\rm a}$, $\mathsf{X}_{\rm b}$ and $\mathsf{X}_{\rm c}$ be uniformly random and independent bits, and define

$$\mathsf{Z}_1 := \mathsf{X}_{\rm a}, \quad \mathsf{Z}_2 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}) \text{ and } \mathsf{Z}_3 := (\mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}). \quad (2.1)$$

Consider 3 users 1, 2 and 3 observing Z_1, Z_2 and Z_3 respectively in private. The private source $(\mathsf{Z}_1, \mathsf{Z}_2, \mathsf{Z}_3)$ is called a PIN [6, 13] in the sense that its statistical dependency can be

The full version of this paper is available on arXiv [1].

C. Chan (email: cchan@inc.cuhk.edu.hk), and Q. Zhou are with the Institute of Network Coding at the Chinese University of Hong Kong, the Shenzhen Key Laboratory of Network Coding Key Technology and Application, China, and the Shenzhen Research Institute of the Chinese University of Hong Kong.

N. Kashyap and M. Mukherjee are with the Department of Electrical Communication Engineering at the Indian Institute of Science, Bangalore.

The work described in this paper was supported by a grant from University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. AoE/E-02/08), and supported partially by a grant from Shenzhen Science and Technology Innovation Committee (JSGG20160301170514984), the Chinese University of Hong Kong (Shenzhen), China.

The work of C. Chan was supported in part by The Vice-Chancellor's One-off Discretionary Fund of The Chinese University of Hong Kong (Project Nos. VCF2014030 and VCF2015007), and a grant from the University Grants Committee of the Hong Kong Special Administrative Region, China (Project No. 14200714).

The work of N. Kashyap and M. Mukherjee was supported in part by a Swarnajayanti Fellowship awarded to N. Kashyap by the Department of Science & Technology (DST), Government of India.

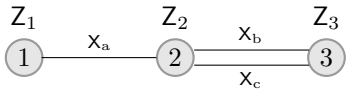

Fig. 1: The graphical representation of the PIN (2.1). Each edge corresponds to an independent random variable observed by the incident nodes.

described by a (multi-)graph as shown in Fig. 1 with the nodes representing the users, X_a represented by an edge incident on nodes 1 and 2, and X_b and X_c represented by two edges incident on nodes 2 and 3.

If user 2 reveals $\mathsf{F} := \mathsf{X}_\mathrm{a} \oplus \mathsf{X}_\mathrm{b}$ in public so that everyone can observe it, then user 3 can recover X_a as $\mathsf{F} \oplus \mathsf{X}_\mathrm{b}$. $\mathsf{K} := \mathsf{X}_\mathrm{a}$ is called a secret key bit generated by the public discussion F because K is not only recoverable by all users but also uniformly random and independent of the public discussion F. A general asymptotic secret key agreement protocol by interactive public discussion was formulated in [2], where the maximum achievable key rate, called the *secrecy capacity* and denoted by C_S, was characterized by a single-letter linear program. For the current example, it is easy to see that $C_\mathrm{S} = 1$, since user 1 observes at most 1 bit in private and 1 bit of secret key is achievable by the above discussion scheme.

A quantity of interest but not characterized in [2] is the smallest public discussion rate required to achieve the secrecy capacity, called the *communication complexity* and denoted by R_S. For the current example, $R_\mathrm{S} \le 1$ because the above capacity-achieving discussion F is 1 bit. However, the precise characterization of R_S has been unknown even for the current simple example.

In this work, we introduce new techniques that not only implies $R_\mathrm{S} = 1$ for the current example but also characterizes the maximum key rate under a total public discussion rate $R \ge 0$, called the rate-constrained secrecy capacity and denoted by $C_\mathrm{S}(R)$. For the current example, it will follow that

$$C_\mathrm{S}(R) = \min\{R, 1\}. \tag{2.2}$$

Although it is easy to see that $C_\mathrm{S}(0) \ge 0$ and $C_\mathrm{S}(R) = 1$, for $R \ge 1$, and that $C_\mathrm{S}(R) \ge \min\{R, 1\}$ by time sharing, proving the reverse inequality is non-trivial and calls for new techniques not covered by [4, 7]. Indeed, our techniques will also imply that only user 2 needs to discuss in public, and so a secret key rate of $r_\mathrm{K} \in [0, 1]$ is achievable by a discussion rate tuple (r_1, r_2, r_3) iff they belong to the region

$$\begin{aligned}\mathscr{R} = \{(r_\mathrm{K}, (r_1, r_2, r_3)) \mid\ & r_\mathrm{K} \in [0,1], \\ & r_1 \ge 0, r_2 \ge r_\mathrm{K}, r_3 \ge 0\}.\end{aligned} \tag{2.3}$$

This matches our intuition, since users 1 and 3 have independent private observations, i.e., Z_1 is independent of Z_3, and so only user 2 can help them share a non-trivial secret key. It turns out that the techniques apply to more general source model with private randomization and interactive discussion allowed as in [2]. It also completely characterizes $C_\mathrm{S}(R)$ for the PIN model.

III. Problem Formulation

We consider the multiterminal secret key agreement [2] without helpers or wiretapper's side information. It involves a finite set $V := [m] := \{1, 2, \dots, m\}$ of $m \ge 2$ users. The users have access to a private (discrete memoryless multiple) source denoted by the random vector

$$\begin{aligned}&\mathsf{Z}_V := (\mathsf{Z}_i | i \in V) \sim P_{\mathsf{Z}_V} \text{ taking values from} \\ &Z_V := \prod\nolimits_{i \in V} Z_i, \text{ assumed to be finite.}\end{aligned}$$

N.b., capital letters in sans serif font are used for random variables and the corresponding capital letters in the usual math italic font denote the alphabet sets. P_{Z_V} denotes the joint distribution of Z_i's. The protocol can be divided into the following phases:

Private observation: Each user $i \in V$ observes an n-sequence

$$\mathsf{Z}_i^n := (\mathsf{Z}_{it} | t \in [n]) = (\mathsf{Z}_{i1}, \mathsf{Z}_{i2}, \dots, \mathsf{Z}_{in})$$

i.i.d. generated from the source Z_i for some block length n.
Private randomization: Each user $i \in V$ generates a random variable U_i independent of the private source, i.e.,

$$H(\mathsf{U}_V | \mathsf{Z}_V) = \sum_{i \in V} H(\mathsf{U}_i). \tag{3.1}$$

For convenience, we denote the entire private observation of user $i \in V$ as

$$\tilde{\mathsf{Z}}_i := (\mathsf{U}_i, \mathsf{Z}_i^n). \tag{3.2}$$

Public discussion: Using a public authenticated noiseless channel, each user $i \in V$ broadcasts a message in round t

$$\mathsf{F}_{it} := f_{it}(\tilde{\mathsf{Z}}_i, \tilde{\mathsf{F}}_{it}) \qquad \text{where} \tag{3.3a}$$
$$\tilde{\mathsf{F}}_{it} := (\mathsf{F}_{[i-1]t}, \mathsf{F}_V^{t-1}), \tag{3.3b}$$

$t \in [\ell]$ for some positive integer ℓ number of rounds, $\mathsf{F}_{[i-1]t}$ consists of the previous messages broadcast in the same round, while F_V^{t-1} denotes the messages broadcast in the previous rounds. Without loss of generality, we assume this interactive discussion is conducted in the ascending order of user indices. We also write

$$\mathsf{F}_i := \mathsf{F}_{i[\ell]} = (\mathsf{F}_{it} | t \in [\ell]) \tag{3.3c}$$
$$\mathsf{F} := \mathsf{F}_V = (\mathsf{F}_i | i \in V) \tag{3.3d}$$

to denote the aggregate message from user $i \in V$ and the aggregation of the messages from all users respectively.
Key generation: A random variable K, called the secret key, is required to satisfy the recoverability constraint that

$$\lim_{n \to \infty} \Pr(\exists i \in V, \mathsf{K} \ne \theta_i(\tilde{\mathsf{Z}}_i, \mathsf{F})) = 0, \tag{3.4}$$

for some function θ_i, and the secrecy constraint that

$$\lim_{n \to \infty} \frac{1}{n} [\log |K| - H(\mathsf{K}|\mathsf{F})] = 0, \tag{3.5}$$

where K denotes the finite alphabet set of possible key values.

Definition 3.1 Given the private source Z_V, a secret key rate r_{K} is achievable by the public discussion rate tuple $r_V := (r_i | i \in V)$ iff

$$r_{\mathrm{K}} \le \liminf_{n\to\infty} \frac{1}{n} \log|K| \text{ and } r_i \ge \limsup_{n\to\infty} \frac{1}{n} \log|F_i|, \quad (3.6)$$

in addition to (3.4) and (3.5). The set of achievable (r_{K}, r_V) is denoted by $\mathscr{R}$. The *rate-constrained secrecy capacity* is defined for $R \ge 0$ as

$$C_{\mathrm{S}}(R) := \max\{r_{\mathrm{K}} \mid (r_{\mathrm{K}}, r_V) \in \mathscr{R}, r(V) \le R\}, \quad (3.7)$$

where, for convenience, $r(B) := \sum_{i\in B} r_i$ for $B \subseteq V$. □

Proposition 3.1 *$C_{\mathrm{S}}(R)$ is continuous, non-decreasing and concave for $R \ge 0$.* □

PROOF Continuity is because the liminf and limsup in (3.6) always exist, since $C_{\mathrm{S}}(R)$ is bounded within $[0, H(\mathsf{Z}_V)]$. The monotonicity is obvious, and concavity follows from the usual time sharing argument. ■

The *unconstrained secrecy capacity* defined and characterized in [2] is the special case

$$\begin{aligned} C_{\mathrm{S}} &:= \lim_{R\to\infty} C_{\mathrm{S}}(R) \quad (3.8)\\ &= C_{\mathrm{S}}(R_{\mathrm{CO}}) = H(\mathsf{Z}_V) - R_{\mathrm{CO}} \end{aligned}$$

where R_{CO} is the *smallest rate of communication for omniscience*, characterzied in [2] by the linear program

$$R_{\mathrm{CO}} = \min\{r(V) \mid r(B) \ge H(\mathsf{Z}_B|\mathsf{Z}_{V\setminus B}), \forall B \subsetneq V\}. \quad (3.9)$$

It was also mentioned in [2] that the unconstrained capacity can be attained by a possibly smaller discussion rate, referred to as the communication complexity

$$\begin{aligned} R_{\mathrm{S}} &:= \min\{r(V) \mid (C_{\mathrm{S}}, r_V) \in \mathscr{R}\} \quad (3.10)\\ &= \min\{R \ge 0 \mid C_{\mathrm{S}}(R) = C_{\mathrm{S}}\} \le R_{\mathrm{CO}}. \end{aligned}$$

Our goal is to characterize or bound $C_{\mathrm{S}}(R)$ and $\mathscr{R}$ using only single-letter expressions. We will also specialize and strengthen the results to the hypergraphical source model:

Definition 3.2 (Definition 2.4 of [8]) Z_V is a *hypergraphical source* w.r.t. a hypergraph (V, E, ξ) with edge functions $\xi : E \to 2^V \setminus \{\emptyset\}$ iff, for some independent (hyper)edge variables X_e for $e \in E$ with $H(\mathsf{X}_e) > 0$,

$$\mathsf{Z}_i := (\mathsf{X}_e \mid e \in E, i \in \xi(e)), \text{ for } i \in V. \quad (3.11)$$

The *weight function* $c : 2^V \setminus \{\emptyset\} \to \mathbb{R}$ of a hypergraphical source is defined as

$$c(B) := H(\mathsf{X}_e \mid e \in E, \xi(e) = B) \text{ with support} \quad (3.12a)$$

$$\mathrm{supp}(c) := \{B \in 2^V \setminus \{\emptyset\} \mid c(B) > 0\} \quad (3.12b)$$

The PIN model [6] such as (2.1) is an example, where the corresponding hypergraph is the graph in Fig. 1 with weight $c(\{1,2\}) = H(\mathsf{X}_{\mathrm{a}}) = 1$, $c(\{2,3\}) = H(\mathsf{X}_{\mathrm{b}}, \mathsf{X}_{\mathrm{c}}) = 2$ and 0 otherwise.

Definition 3.3 ([6]) Z_V is a PIN iff it is hypergraphical w.r.t. a graph (V, E, ξ) with edge function $\xi : E \to V^2 \setminus \{(i,i) \mid i \in V\}$ (i.e., no self loops). □

For this special source model, there is a protocol in [13, Proof of Theorem 3.3] that achieves the unconstrained secrecy capacity [13, (15),(17)].

Proposition 3.2 ([6, 13]) *For a PIN with weight c, there is a secret key agreement scheme, called the* tree-packing protocol*, which achieves $(r_{\mathrm{K}}, r_V) \in \mathscr{R}$ with*

$$r_{\mathrm{K}} := \sum_{j\in[k]} \eta_j \text{ and } r_i := \sum_{j\in[k]} (d_{T_j}(i) - 1)\eta_j \text{ for } i \in V, \quad (3.13a)$$

where k is a non-negative integer; $\eta_j \in \mathbb{R}_+$ is a non-negative real number; $T_j := (V, \mathcal{E}_j)$ is a spanning tree with edge set $\mathcal{E}_j \subseteq V^2 \setminus \{(i,i) \mid i \in V\}$ satisfying

$$\sum_{j\in[k]: B\in\mathcal{E}_j} \eta_j \le c(B) \quad \forall B \in 2^V \setminus \{\emptyset\}, \quad (3.13b)$$

which is the constraint for fractional tree-packing [14]; and $d_{T_j}(i)$ is the degree of node i in T_j. Furthermore, the unconstrained secrecy capacity C_{S} is the maximum r_{K} over the fractional tree packing $\{(\eta_j, T_j) \mid i \in [k]\}$. □

However, it was left as an open problem in [6] whether the above scheme achieves R_{S}. We resolve this in the affirmative by providing a matching converse.

IV. Main Results

We will make use of the following alternative characterization of the unconstrainted secrecy capacity in [8]: For the no-helper case, $C_{\mathrm{S}} = I(\mathsf{Z}_V)$ where $I(\mathsf{Z}_V)$ is called the multivariate mutual information (MMI) defined as

$$I(\mathsf{Z}_V) := \min_{\mathcal{P}\in\Pi'(V)} I_{\mathcal{P}}(\mathsf{Z}_V), \text{ with} \quad (4.1a)$$

$$I_{\mathcal{P}}(\mathsf{Z}_V) := \frac{1}{|\mathcal{P}| - 1} \Big[\underbrace{\sum\nolimits_{C\in\mathcal{P}} H(\mathsf{Z}_C) - H(\mathsf{Z}_V)}_{= D(P_{\mathsf{Z}_V} \| \prod_{C\in\mathcal{P}} P_{\mathsf{Z}_C})} \Big] \quad (4.1b)$$

and $\Pi'(V)$ being the set of partitions of V into at least 2 non-empty disjoint subsets of V. The conditional versions $I(\mathsf{Z}_V|\mathsf{W}')$ and $I_{\mathcal{P}}(\mathsf{Z}_V|\mathsf{W}')$ are defined in the same way but with the entropy terms conditioned on W' in addition. $D(\cdot\|\cdot)$ is the Kullback–Leibler divergence, which is non-negative, and so are I and $I_{\mathcal{P}}$. It was pointed out in [5] that the set of optimal solutions form a lattice w.r.t. the partial order $\mathcal{P}' \succeq \mathcal{P}$ iff

$$\forall C \in \mathcal{P}, \exists C' \in \mathcal{P}' : C \subseteq C'.$$

Hence, there exists a unique finest optimal partition, denoted by $\mathcal{P}^*(\mathsf{Z}_V)$ and referred to as the fundamental partition. Furthermore, both the MMI and the optimal partitions can be computed in strongly polynomial time w.r.t. the number of evaluation of the entropies.

In the bivariate case when $V = \{1, 2\}$, the MMI reduces to Shannon's mutual information

$$I(\mathsf{Z}_{\{1,2\}}) = I(\mathsf{Z}_1 \wedge \mathsf{Z}_2) = H(\mathsf{Z}_1) + H(\mathsf{Z}_2) - H(\mathsf{Z}_1, \mathsf{Z}_2),$$

because $\{\{1\},\{2\}\}$ is the unique partition in $\Pi'(\{1,2\})$ (and is therefore the fundamental partition $\mathcal{P}^*(\mathsf{Z}_{\{1,2\}})$).

We begin with some general lower bounds on the public discussion rates:

Theorem 4.1 *For any $(r_{\mathrm{K}}, r_V) \in \mathscr{R}$, we have*

$$r(V \setminus B) \geq (|\mathcal{P}| - 1)[r_{\mathrm{K}} - I_{\mathcal{P}}(\mathsf{Z}_B)] \tag{4.2}$$

for any $B \subseteq V$ with size $|B| > 1$ and $\mathcal{P} \in \Pi'(B)$. □

PROOF See the full version [1] of the paper. ■

(4.2) is a lower bound on the total discussion rate $r(V \setminus B)$ of the subset $V \setminus B$ of users required to achieve a secret key rate of r_{K}, for any choice of subset B of more than one user. Choosing $\mathcal{P}$ to be the fundamental partition $\mathcal{P}^*(\mathsf{Z}_B)$ in (4.2), $I_{\mathcal{P}}(\mathsf{Z}_B) = I(\mathsf{Z}_B)$, which gives the following lower bound in terms of the MMI.

Corollary 4.1 *For any $(r_{\mathrm{K}}, r_V) \in \mathscr{R}$, we have*

$$r(V \setminus B) \geq (|\mathcal{P}^*(\mathsf{Z}_B)| - 1)[r_{\mathrm{K}} - I(\mathsf{Z}_B)] \tag{4.3}$$

for any $B \subseteq V$ with size $|B| > 1$. □

Note that $I(\mathsf{Z}_B)$ in (4.3) is the secrecy capacity when users in $V \setminus B$ are removed. Hence, to achieve a secret key rate beyond $I(\mathsf{Z}_B)$, users in $V \setminus B$ must discuss. (4.3) states that the total discussion rate of users in $V \setminus B$ is at least the additional secret key rate $r_{\mathrm{K}} - I(\mathsf{Z}_B)$ amplified by a factor of $|\mathcal{P}^*(\mathsf{Z}_B)| - 1 \geq 1$.

Applying (4.2) to the example in Section II with $B = \{1,3\}, \mathcal{P} = \{\{1\},\{3\}\}$ (or simply (4.3)), we have

$$r_2 \geq (2-1)[r_{\mathrm{K}} - I(\mathsf{Z}_1 \wedge \mathsf{Z}_3)] = r_{\mathrm{K}} \tag{4.4}$$

This is achievable as mentioned in Section II by time sharing between $(r_{\mathrm{K}}, (r_1, r_2, r_3)) = (0, (0,0,0))$ and $(1, (0,1,0)) \in \mathscr{R}$. Since $C_{\mathrm{S}} = I(\mathsf{Z}_{\{1,2,3\}}) \leq I(\mathsf{Z}_{\{1,2\}} \wedge \mathsf{Z}_3) = 1$ and is achievable, we have (2.3) as the achievable rate region $\mathscr{R}$. More generally,

Theorem 4.2 *For PIN with weight c such that $\mathrm{supp}(c)$, defined in (3.12), forms a spanning tree, we have*

$$\mathscr{R} = \{(r_{\mathrm{K}}, r_V) \mid r_{\mathrm{K}} \in [0, C_{\mathrm{S}}], \; r_i \geq (d(i) - 1)\, r_{\mathrm{K}}, i \in V\}, \quad \textit{where} \tag{4.5a}$$

$$C_{\mathrm{S}} = \min\{c(\{i,j\}) \mid \{i,j\} \in \mathrm{supp}(c)\}, \tag{4.5b}$$

and $d(i)$ is the degree of node i in the spanning tree. □

PROOF Since the source model forms a Markov tree w.r.t. the spannnig tree given by $\mathrm{supp}(c)$, the unconstrained secrecy capacity (4.5b) follows from [2, (36)].

To prove (4.5a), consider any PIN with weight function c such that $\mathrm{supp}(c)$ forms a spanning tree. For any $i \in V$, choose $B = V \setminus \{i\}$ and let $\mathcal{P}$ be the connected components of the spanning tree after node i and its incident edges are removed. It follows that $\mathcal{P} \in \Pi'(B)$ with

$$|\mathcal{P}| = d(i) \quad \text{and} \quad I_{\mathcal{P}}(\mathsf{Z}_B) = 0$$

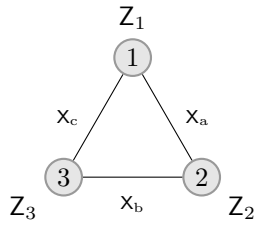

Fig. 2: The triangle PIN defined in (4.6).

due to the fact that $\mathrm{supp}(c)$ forms a spanning tree. By (4.1) in Theorem 4.2, we have

$$r_i \geq (|\mathcal{P}| - 1)\,[r_{\mathrm{K}} - I_{\mathcal{P}}(\mathsf{Z}_B)] = (d(i) - 1)\, r_{\mathrm{K}}.$$

The lower bound is achievable by Proposition 3.2, hence completing the proof of (4.5a). ■

The current example has a weight function c with

$$\mathrm{supp}(c) = \{\{1,2\},\{2,3\}\},$$

which is a spanning tree with node degrees given by

$$d(1) = d(3) = 1 \quad \text{and} \quad d(2) = 2,$$

which gives the lower bound (4.4) and hence the region in (2.3). The capacity is the minimum edge weight, i.e.,

$$C_{\mathrm{S}} = \min\{c(\{1,2\}), c(\{2,3\})\} = \min\{1,2\} = 1.$$

Unfortunately, the lower bound (4.2) can be loose for PIN with cycles. E.g., consider a triangle PIN with $V := [3]$ and

$$\mathsf{Z}_1 := (\mathsf{X}_{\mathrm{a}}, \mathsf{X}_{\mathrm{c}}), \;\; \mathsf{Z}_2 := (\mathsf{X}_{\mathrm{a}}, \mathsf{X}_{\mathrm{b}}) \;\text{ and }\; \mathsf{Z}_3 := (\mathsf{X}_{\mathrm{b}}, \mathsf{X}_{\mathrm{c}}) \tag{4.6}$$

where $\mathsf{X}_{\mathrm{a}}, \mathsf{X}_{\mathrm{b}}, \mathsf{X}_{\mathrm{c}}$ are independent uniformly random bits. This a PIN with correlation represented by a triangle in Fig. 2. It follows from (3.8), (3.9) and (3.10) that

$$C_{\mathrm{S}} = R_{\mathrm{CO}} = 1.5 \geq R_{\mathrm{S}}.$$

In particular, the secret key rate of 1 is achievable by the scheme described in Section II.

Applying (4.2) with $B = \{1,3\}$ and $\mathcal{P} = \{\{1\},\{3\}\}$ again,

$$r_2 \geq r_{\mathrm{K}} - I(\mathsf{Z}_1 \wedge \mathsf{Z}_3) = r_{\mathrm{K}} - 1.$$

This is the best possible bound involving r_2 over all possible choices of B and $\mathcal{P}$, but it is trivial when $r_{\mathrm{K}} \leq 1$. By symmetry, the best bounds for r_1 and r_3 are also trivial when $r_{\mathrm{K}} \leq 1$.

Nevertheless, we discovered a different bounding technique that can give a non-trivial bound in the above case, by exploiting the hypergraphical dependency structure of the source:

Theorem 4.3 *For hypergraphical source, we have $(r_{\mathrm{K}}, r_V) \in \mathscr{R}$ only if*

$$\alpha(\mathcal{P}) r(V) \geq [1 - \alpha(\mathcal{P})]\, r_{\mathrm{K}} \quad \forall \mathcal{P} \in \Pi'(V), \quad \textit{where} \tag{4.7a}$$

$$\alpha(\mathcal{P}) := \frac{\max_{e \in E} |\{C \in \mathcal{P} \mid C \cap \xi(e) \neq \emptyset\}| - 1}{|\mathcal{P}| - 1} \tag{4.7b}$$

and ξ is the edge function of the hypergraph in (3.11). □

N.b., it is easy to see that $\alpha(\mathcal{P}) \in [0,1]$ because the maximization in the numerator of (4.7b) is the maximum number of blocks in $\mathcal{P}$ that an edge $e \in E$ can intersect, which is between 1 and $|\mathcal{P}|$. If $\alpha(\mathcal{P}) = 0$ for some $\mathcal{P} \in \Pi'(V)$, then (4.7a) becomes $r_K \leq 0$, i.e., $C_{\rm S} = 0$. This happens when no edge crosses $\mathcal{P}$, i.e., the source corresponds to a disconnected hypergraph.

PROOF See the full version [1] of the paper. ∎

For the current example, choose $\mathcal{P} = \{\{1\},\{2\},\{3\}\}$. For each edge e, $\Big|\{C \in \mathcal{P} | C \cap \xi(e) \neq \emptyset\}\Big|$ simplifies to the number of incident nodes, which is always 2 for graphs. Hence,

$$\alpha(\mathcal{P}) = \frac{2-1}{3-1} = 0.5 \quad \text{and so} \quad r(V) \geq \frac{1-0.5}{0.5} r_{\rm K} = r_{\rm K}.$$

Since $C_{\rm S} = R_{\rm CO} = 1.5$, the lower bound above is achievable by time-sharing, which gives

$$C_{\rm S}(R) = \min\{R, 1.5\} \quad \text{and so} \quad R_{\rm S} = 1.5.$$

Surprisingly, the argument can be extended to any PIN for a complete characterization of the communication complexity as well as the rate-constrained secrecy capacity.

Theorem 4.4 *For PIN,*

$$C_{\rm S}(R) = \min\left\{\frac{R}{|V|-2}, C_{\rm S}\right\}, \tag{4.8}$$

which gives $R_{\rm S} = (|V|-2)C_{\rm S}$. □

PROOF The converse follows from (4.7a) with $\mathcal{P} = \{\{i\} | i \in V\}$. More precisely, the minimization in the numerator of $\alpha(\mathcal{P})$ is always equal to 2 as it is the number of incident nodes of an edge. Hence,

$$\alpha(\mathcal{P}) = \frac{1}{|V|-1} \quad \text{and so} \quad r(V) \geq (|V|-2) r_{\rm K}$$

by (4.7a). The lower bound can be shown to be achievable by Proposition 3.2. With $(r_{\rm K}, r_V)$ defined in (3.13a),

$$r(V) = \sum_{i \in V} \sum_{j=1}^{k} [d_{T_j}(i) - 1]\eta_j = \sum_{j=1}^{k} \eta_j \sum_{i \in V} [d_{T_j}(i) - 1]$$

which simplifies to $(|V|-2)r_{\rm K}$ as desired using the fact that $\sum_{i \in V} d_{T_j}(i) = |\mathcal{E}_j| = |V| - 1$ as T_j is a spanning tree. ∎

V. Extensions and Challenges

While the lower bound (4.2) can be loose in the presence of cycles, it can be shown to be tight for hypergraphical sources that correspond to hypergraphs that are minimally connected in the sense that removing any edge disconnects the hypergraph. This generalizes the result of Theorem 4.2 from PINs to hypergraphical sources. Both lower bounds (4.2) and (4.7) can also be extended to include helpers. However, it is unclear how one can generalize (4.7) to more general sources that are possibly non-hypergraphical. Another interesting open problem is to characterize $\mathscr{R}$ for PINs with cycles, thereby improving Theorem 4.2 to allow for cycles.

The bound in (4.7) can be loose for hypergraphical sources. A trivial example is where $V := [3]$ and

$$\mathsf{Z}_1 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm c}), \quad \mathsf{Z}_2 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}) \quad \text{and} \quad \mathsf{Z}_3 := (\mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}).$$

The numerator of $\alpha(\mathcal{P})$ in (4.7b) is 0 for any $\mathcal{P}$, as the mininum is achieved by the hyperedge c incident on all the nodes. Hence, $\alpha(\mathcal{P}) = 0$ and so (4.7) becomes trivial. However, with $B = \{1,3\}$ and $\mathcal{P} = \{\{1\},\{3\}\}$, (4.2) gives $r_2 \geq r_{\rm K} - 1$, which is non-trivial for $1 < r_{\rm K} \leq 2 = C_{\rm S}$. We also conjecture that (4.2) and (4.7) are both loose for the example where $V := [6]$ and

$$\mathsf{Z}_1 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm d}), \quad \mathsf{Z}_2 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm b}), \quad \mathsf{Z}_3 := (\mathsf{X}_{\rm a}, \mathsf{X}_{\rm b}, \mathsf{X}_{\rm d})$$
$$\mathsf{Z}_4 := (\mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}, \mathsf{X}_{\rm d}), \quad \mathsf{Z}_5 := (\mathsf{X}_{\rm b}, \mathsf{X}_{\rm c}) \quad \text{and} \quad \mathsf{Z}_6 := \mathsf{X}_{\rm c}.$$

We conjecture that $(r_{\rm K}, r_V) \in \mathscr{R}$ only if $r(V) \geq 1.5 r_{\rm K}$, which is achievable using the idea of secret key agreement by network coding [8]. It can be shown that the best lower bound from (4.2) and (4.7) is $r(V) \geq r_{\rm K}$. Hence, we expect that resolving the conjecture in the affirmative potentially leads to new techniques for obtaining better lower bounds on the public discussion rate required for secret key agreement.

References

[1] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "Secret key agreement under discussion rate constraints," *arXiv preprint arXiv:1701.05008*, 2017. [Online]. Available: http://arxiv.org/abs/1701.05008

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

[3] H. Tyagi, "Common information and secret key capacity," *IEEE Transactions on Information Theory*, vol. 59, no. 9, pp. 5627–5640, Sept 2013.

[4] 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.

[5] 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.

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

[7] C. Chan, M. Mukherjee, N. Kashyap, and Q. Zhou, "When is omniscience a rate-optimal strategy for achieving secret key capacity?" in *2016 IEEE Information Theory Workshop (ITW)*, Sept 2016, pp. 354–358.

[8] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," in *Proceedings of 44th Annual Conference on Information Sciences and Systems*, 2010.

[9] C. Chan, A. Al-Bashabsheh, and Q. Zhou, "Incremental and decremental secret key agreement," in *Proc. IEEE Int. Symp. on Inf. Theory*, July 2016, pp. 2514–2518.

[10] 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 *Proc. IEEE Int. Symp. on Inf. Theory*, July 2016, pp. 2504–2508.

[11] J. Liu, P. W. Cuff, and S. Verdú, "Common randomness and key generation with limited interaction," *CoRR*, vol. abs/1601.00899, 2016.

[12] A. Kaspi, "Two-way source coding with a fidelity criterion," *IEEE Trans. Inf. Theory*, vol. 31, pp. 735–740, Nov. 1985.

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

[14] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*. Springer, 2002.