entropy

MDPI

Article

Compressed Secret Key Agreement: Maximizing Multivariate Mutual Information per Bit

Chung Chan

Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong, China; chungc@alum.mit.edu

Received: 5 July 2017; Accepted: 3 October 2017; Published: 14 October 2017

Abstract: The multiterminal secret key agreement problem by public discussion is formulated with an additional source compression step where, prior to the public discussion phase, users independently compress their private sources to filter out strongly correlated components in order to generate a common secret key. The objective is to maximize the achievable key rate as a function of the joint entropy of the compressed sources. Since the maximum achievable key rate captures the total amount of information mutual to the compressed sources, an optimal compression scheme essentially maximizes the multivariate mutual information per bit of randomness of the private sources, and can therefore be viewed more generally as a dimension reduction technique. Single-letter lower and upper bounds on the maximum achievable key rate are derived for the general source model, and an explicit polynomial-time computable formula is obtained for the pairwise independent network model. In particular, the converse results and the upper bounds are obtained from those of the related secret key agreement problem with rate-limited discussion. A precise duality is shown for the two-user case with one-way discussion, and such duality is extended to obtain the desired converse results in the multi-user case. In addition to posing new challenges in information processing and dimension reduction, the compressed secret key agreement problem helps shed new light on resolving the difficult problem of secret key agreement with rate-limited discussion by offering a more structured achieving scheme and some simpler conjectures to prove.

Keywords: secret key agreement; source compression; rate-limited discussion; communication complexity; dimension reduction; multivariate mutual information

1. Introduction

In information-theoretic security, the problem of secret key agreement by public discussion concerns a group of users discussing in public to generate a common secret key that is independent of their discussion. The problem was first formulated by Maurer [1] and Ahlswede and Csiszár [2] under a private source model involving two users who observe some correlated private sources. Rather surprisingly, public discussion was shown to be useful in generating the secret key; i.e., it strictly increases the maximum achievable secret key rate, called the *secrecy capacity*. This phenomenon was also discovered in [3] in a different formulation. Furthermore, the secrecy capacity was given an information-theoretically appealing characterization—it is equal to Shannon's mutual information [4] between the two private sources, assuming the wiretapper can listen to the entire public discussion but not observe any other side information of the private sources. It was also shown that the capacity can be achieved by one-way public discussion (i.e., with only one of the users discussing in public).

As a simple illustration, let X_0, X_1, and J be three uniformly random independent bits, and suppose user 1 observes $Z_1 := (X_0, X_1)$ privately while user 2 observes $Z_2 := (X_J, J)$, where $X_J = X_0$ when $J = 0$ but $X_J = X_1$ when $J = 1$. If user 2 reveals J in public, then user 1 can recover X_J and therefore Z_2. Furthermore, since X_J is independent of J, it can serve as a secret key bit that is recoverable by both users but remains perfectly secret to a wiretapper who observes only the public message

J. This scheme achieves a secrecy capacity equal to the mutual information $I(\mathsf{Z}_1 \wedge \mathsf{Z}_2) = 1$ roughly because user 2 reveals $H(\mathsf{Z}_2|\mathsf{Z}_1) = 1$ bit in public so there is $H(\mathsf{Z}_2) - H(\mathsf{Z}_2|\mathsf{Z}_1) = I(\mathsf{Z}_1 \wedge \mathsf{Z}_2)$ bits of randomness left for the secret key. However, if no public discussion is allowed, it follows from the work of Gác and Körner [5] that no common secret key bit can be extracted from the sources. In particular, X_J cannot be used as a secret key because user 1 does not know whether X_J is X_0 or X_1. X_0 andX_1 cannot be used as a secret key either because they may not be observed by user 2 when $\mathsf{J} = 1$ and $\mathsf{J} = 0$, respectively. It can be seen that while the private sources are clearly statistically dependent, public discussion is needed to consolidate the mutual information of the sources into a common secret key.

The secret key agreement formulation was subsequently extended to the multi-user case by Csiszár and Narayan [6]. Some users are also allowed to act as *helpers* who can participate in the public discussion but need not share the secret key. The designated set of users who need to share the secret key are referred to as the *active users*. In contrast to the two-user case, one-way discussion may not achieve the secrecy capacity when there are more than two users. Instead, an *omniscience strategy* was considered in [6] in which the users first communicate minimally in public until omniscience; that is, the users discuss in public at the smallest total rate until every active user can recover all the private sources. The scheme was shown to achieve the secrecy capacity in the case when the wiretapper only listens to the public discussion. However, this assumes that the public discussion is lossless and unlimited in rate, and the sources take values from finite alphabet sets. If the sources are continuous or if the public discussion is limited to a certain rate, it may be impossible to attain omniscience.

This work is motivated by the search for a better alternative to the omniscience strategy for multiterminal secret key agreement. A prior work of Csiszár and Narayan [7] considered secret key agreement under rate-limited public discussion. The model involves two users and a helper observing correlated discrete memoryless sources. The public discussion of the users is conducted in a particular order and direction. While the region of achievable secret key rate and discussion rates remains unknown, single-letter characterizations involving two auxiliary random variables were given for many special cases, including the two-user case with two rounds of interactive public discussion, where each user speaks once in sequence, with the last public message possibly depending on the first. By further restricting to one-way public discussion, the characterization involves only one auxiliary random variable and was extended to continuous sources by Watanabe and Oohama in [8], where they also gave an explicit characterization without any auxiliary random variable for scalar Gaussian sources in [8]. For vector Gaussian sources, the characterization by the same authors in [9] involving some matrix optimization was further improved in [10] to a more explicit formula. However, if the discussion is allowed to be two-way and interactive, Tyagi [11] showed with a concrete two-user example that the minimum total discussion rate required—called the *communication complexity*—can be strictly reduced. Using the technique of Kaspi [12], multi-letter characterizations were given in [11] for the communication complexity, and similarly by Liu et al. in [13] for the region of achievable secret key rate. The characterization was further simplified in [13] using the idea of convex envelope using the technique by Ma et al. [14]. While these characterizations provide many new insights and properties, they are not considered computable compared to the usual single-letter and explicit characterizations. Further extension to the multi-user case also appears difficult, as the converse can be seen to rely on the Csiszár sum identity [2] (Lemma 4.1), which does not appear to extend beyond the two-user case.

Nevertheless, partial solutions under more restrictive public discussion constraints were possible. By simplifying the problem to the right extent, new results were discovered in the multi-user case, which has led to the formulation in this work. For instance, Gohari and Anantharam [15] characterized the secrecy capacity in the multi-user case under the simpler vocality constraint where some users have to remain silent throughout the public discussion. Using this result, simple necessary and sufficient conditions can be derived as to whether a user can remain silent without diminishing the maximum achievable key rate [16–18]. This is a simpler result than characterizing the achievable rate region because it does not say how much discussion is required if a user must discuss. Another line

of work [19–22] follows [11] to characterize the communication complexity, but in the multi-user case. Courtade and Halford [19] characterized the communication complexity under a special non-asymptotic hypergraphical source model with linear discussion. A multi-letter lower bound was obtained in [21] for the communication complexity for the asymptotic general source model. It also gave a precise and simple condition under which the omniscience strategy for secret key agreement is optimal for a special source model called the *pairwise independent network (PIN)* [23], which is a special hypergraphical source model [24]. In [22,25], some single-letter and more easily computable explicit lower bounds were also derived. These bounds also lead to conditions for the omniscience strategy to be optimal under the hypergraphical source model, which covers the PIN model as a special case. The more general problem of characterizing the multiterminal secrecy capacity under rate-limited public discussion was considered in [26]. In particular, an objective of [26] is to characterize the *constrained secrecy capacity*, defined as the maximum achievable key rate as a function of the total discussion rate. This covers the communication complexity as a special case when further increase in the public discussion rate does not increase the secrecy capacity. While only single-letter bounds were derived for the general source model, a surprisingly simple explicit formula was derived for the PIN model [26]. The optimal scheme in [26] follows the tree-packing protocol in [27]. It turns out to belong to the more general approach of decremental secret key agreement in [28,29] inspired by the achieving scheme in [19] and the notion of excess edge in [24]. More precisely, the omniscience strategy is applied after some excess or less-useful edge random variables are removed (decremented) from the source. Because the entropy of the decremented source is smaller, the discussion required to attain omniscience of the decremented source is also less. Such decremental secret key agreement approach applies to hypergraphical sources more generally, and it results in one of the best upper bounds in [20] for communication complexity. However, for more general source models that are not necessarily hypergraphical, the approach does not directly apply.

The objective of this work is to formalize and extend the idea of decremental secret key agreement beyond the hypergraphical source model. More precisely, the secret key agreement problem is considered with an additional source compression step before public discussion, in which each user independently compresses their private source component to filter away less correlated randomness that does not contribute much to the achievable secret key rate. The compression is such that the entropy rate of the compressed sources is reduced to under a certain specified level. In particular, the edge removal process in decremental secret key agreement can be viewed as a special case of source compression, and the more general problem is referred to as *compressed secrecy key agreement*. The objective is to characterize the achievable secret key rate maximized over all valid compression schemes. For simplicity, this work will focus on the case without helpers—that is, when all users are active and want to share a common secret key. A closely related formulation is given by Nitinawarat and Narayan [30], which characterized the maximum achievable key rate for the two-user case under the scalar Gaussian source model where one of the users is required to quantize the source to within a given rate. The formulation and techniques in [30] was also extended in [31] to the multi-user case where every user can quantize their sources individually to a certain rate. The compression considered in this work is more general than quantizations for Gaussian sources, and the new results are meaningful beyond continuous sources.

The compressed secret key agreement problem is also motivated by the study of multivariate mutual information (MMI) [32]—that is, an extension of Shannon's mutual information to the multivariate case involving possibly more than two random variables. The unconstrained secrecy capacity in the no-helper case has been viewed as a measure of mutual information in [32,33], not only because of its mathematically appealing interpretations such as the residual independence relation and data processing inequalities in [32], but also because of its operational significance in undirected network coding [34,35], data clustering [36], and feature selection [37] (cf. [38]). The optimal source compression scheme that achieves the compressed secrecy capacity can be viewed more generally as an optimal dimension reduction procedure that maximizes the MMI per bit of randomness, which is

an extension of the information bottleneck problem [39] to the multivariate case. However, different from the multivariate extension in [40], the MMI is used instead of Watanabe's total correlation [41], and so it captures only the information mutual to all the random variables rather than the information mutual to any subsets of the random variables. Furthermore, the compression is on each random variable rather than subsets of random variables.

The paper is organized as follows. The problem of compressed secret key agreement is formulated in Section 2. Preliminary results of the secret key agreement are given in Section 3. The main results are motivated in Section 4 and presented in Section 5, followed by the conclusion and some discussions on potential extensions in Section 6.

2. Problem Formulation

Similarly to the multiterminal secret key agreement problem [6] without helpers or wiretappers' side information, the setting of the problem involves a finite set V of $|V| > 1$ users, and a discrete memoryless multiple source:

$$\begin{aligned} &\mathsf{Z}_V := (\mathsf{Z}_i | i \in V) \sim P_{\mathsf{Z}_V} \text{ taking values from} \\ &Z_V := \textstyle\prod_{i \in V} Z_i \quad \text{(not necessarily finite).} \end{aligned}$$

Note that 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.

A secret key agreement protocol with source compression can be broken into the following phases:

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

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

i.i.d. generated from the source Z_i for some block length n. For convenience, $[n]$ denotes the set of positive integers up to n (i.e., $\{1, \ldots, n\}$).

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

$$H(\mathsf{U}_V | \mathsf{Z}_V) = \sum_{i \in V} H(\mathsf{U}_i). \tag{1}$$

- Source compression: Each user $i \in V$ computes

$$\tilde{\mathsf{Z}}_i = \zeta_i(\mathsf{U}_i, \mathsf{Z}_i^n) \tag{2}$$

for some function ζ_i that maps to a finite set. $\tilde{\mathsf{Z}}_V$ is referred to as the compressed source.

- Public discussion: Using a public authenticated noiseless channel, a user $i_t \in V$ is chosen in round $t \in [\ell]$ to broadcast a message

$$\tilde{\mathsf{F}}_t := \tilde{f}_t(\tilde{\mathsf{Z}}_{i_t}, \tilde{\mathsf{F}}^{t-1}) \quad \text{where} \tag{3a}$$

ℓ is a positive integer denoting the number of rounds and $\tilde{\mathsf{F}}^{t-1}$ denotes all the messages broadcast in the previous rounds. If the dependency on $\tilde{\mathsf{F}}^{t-1}$ is dropped, the discussion is said to be *non-interactive*. The discussion is said to be one-way (from user i) if $\ell = 1$ (and $i_1 = 1$). For convenience,

$$\mathsf{F}_i := (\tilde{\mathsf{F}}_t | t \in [\ell], i_t = i) \tag{3b}$$

$$\mathsf{F} := \tilde{\mathsf{F}}^{\ell} = \mathsf{F}_V \tag{3c}$$

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

$$\lim_{n\to\infty} \Pr(\exists\, i \in V, \mathsf{K} \neq \theta_i(\tilde{\mathsf{Z}}_i, \mathsf{F})) = 0, \tag{4}$$

for some function θ_i, and the secrecy constraint:

$$\lim_{n\to\infty} \frac{1}{n} [\log|K| - H(\mathsf{K}|\mathsf{F})] = 0, \tag{5}$$

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

Note that, unlike [11], non-interactive discussion is considered different from one-way discussion in the two-user case, since both users are allowed to discuss even though their messages cannot depend on each other. In contrast to [42], there is an additional source compression phase, after which the protocol can only depend on the original sources through the compressed sources.

The objective is to characterize the maximum achievable secret key rate for a continuum of different levels of source compression:

Definition 1. *The* compressed secrecy capacity *with a joint entropy limit $\alpha \geq 0$ is defined as*

$$\tilde{C}_{\mathrm{S}}(\alpha) := \sup \liminf_{n\to\infty} \frac{1}{n} \log|K| \tag{6}$$

where the supremum is over all possible compressed secret key agreement schemes satisfying

$$\limsup_{n\to\infty} \frac{1}{n} H(\tilde{\mathsf{Z}}_V) - \alpha \leq 0. \tag{7}$$

This constraint limits the joint entropy rate of the compressed source.

Note that instead of the joint entropy limit, one may also consider entropy limits on some subset $B \subseteq V$ that

$$\limsup_{n\to\infty} \frac{1}{n} H(\tilde{\mathsf{Z}}_B) - \alpha \leq 0. \tag{8}$$

If multiple entropy limits are imposed, $\tilde{C}_{\mathrm{S}}$ will be a higher-dimensional surface instead of a one-dimensional curve. For example, in the two-user case under the scalar Gaussian source model, the entropy limit was imposed on only one of the users in [30]. In [31], the multi-user case under the Gaussian Markov tree model was considered under the symmetric case where the entropy limit is imposed on every user.

However, for simplicity, the joint entropy constraint (7) will be the primary focus in this work. It will be shown that $\tilde{C}_S(\alpha)$ is closely related to the *constrained secrecy capacity* $C_S(R)$ defined as [26]:

$$C_S(R) := \sup \liminf_{n\to\infty} \frac{1}{n} \log|K| \quad \text{for } R \geq 0, \tag{9}$$

with $\tilde{Z}_i := (U_i, Z_i^n)$ instead of (2) (i.e., without compression), and the entropy limit (7) replaced by the constraint on the total discussion rate:

$$R \geq \limsup_{n\to\infty} \frac{1}{n} \log|F| = \limsup_{n\to\infty} \frac{1}{n} \sum_{i\in V} \log|F_i|. \tag{10}$$

It follows directly from the result of [6] that $\tilde{C}_S(\alpha)$ remains unchanged whether or not the discussion is interactive. Indeed, the relation between $\tilde{C}_S(\alpha)$ and $C_S(R)$ to be shown in this work will not be affected either. Therefore, for notational simplicity, $C_S(R)$ may refer to the case with or without interaction, even though $C_S(R)$ may be smaller with non-interactive discussion.

It is easy to show that $C_S(R)$ is continuous, non-decreasing, and concave in R [26] (Proposition 3.1). As R goes to ∞, the secrecy capacity

$$C_S(\infty) := \liminf_{R\to\infty} C_S(R) \tag{11}$$

is the usual *unconstrained secrecy capacity* defined in [6] without the discussion rate constraint (10). The smallest discussion rate that achieves the unconstrained secrecy capacity is the *communication complexity* denoted by

$$R_S := \inf\{R \geq 0 \mid C_S(R) = C_S(\infty)\}. \tag{12}$$

Similar to $C_S(R)$, the following basic properties can be shown for $\tilde{C}_S(\alpha)$:

Proposition 1. *$\tilde{C}_S(\alpha)$ is continuous, non-decreasing, and concave in $\alpha \geq 0$. Furthermore,*

$$C_S(\infty) = \liminf_{\alpha\to\infty} \tilde{C}_S(\alpha), \tag{13}$$

achieving the unconstrained secrecy capacity in the limit.

Proof. Continuity, monotonicity, and (13) follow directly from the definition of $\tilde{C}_S(\alpha)$. Concavity follows from the usual time-sharing argument; i.e., for any $\lambda \in [0,1]$, $\alpha', \alpha'' > 0$, a secret key rate of $\lambda\tilde{C}_S(\alpha') + (1-\lambda)\tilde{C}_S(1-\alpha')$ is achievable with the entropy limit $\alpha := \lambda\alpha' + (1-\lambda)\alpha''$ by applying the optimal scheme that achieves $\tilde{C}_S(\alpha')$ for the first $n' := \lfloor \lambda n \rfloor$ samples of Z_V^n and applying the optimal scheme that achieves $\tilde{C}_S(\alpha'')$ for the remaining $n'' := n - n'$ samples. □

Because of (13), a quantity playing the same role of R_S for C_S can be defined for $\tilde{C}_S(\alpha)$ as follows.

Definition 2. *The smallest entropy limit that achieves the unconstrained secrecy capacity is defined as*

$$\alpha_S := \inf\{\alpha \mid \tilde{C}_S(\alpha) = C_S(\infty)\} \tag{14}$$

and referred to as the minimum admissible joint entropy.

One may also consider both the entropy limit (7) and discussion rate constraint (10) simultaneously, and define the secrecy capacity as a function of α and R. However, for simplicity, we will not consider this case but instead focus on the relationship between $\tilde{C}_S(\alpha)$ and $C_S(R)$.

The following example illustrates the problem formulation. It will be revisited at the end of Section 5 (Example 3) to illustrate the main results.

Example 1. *Consider* $V := \{1,2,3\}$ *and*

$$\mathsf{Z}_1 := (\mathsf{X}_a, \mathsf{X}_b), \quad \mathsf{Z}_2 := (\mathsf{X}_a, \mathsf{X}_b, \mathsf{X}_c), \quad \text{and} \quad \mathsf{Z}_3 := (\mathsf{X}_a, \mathsf{X}_c), \tag{15}$$

where $\mathsf{X}_a, \mathsf{X}_b$, *and* X_c *are uniformly random and independent bits. It is easy to argue that*

$$\tilde{C}_{\mathsf{S}}(\alpha) \geq \alpha \quad \text{for } \alpha \in [0,1]. \tag{16a}$$

To see this, notice that X_a *is observed by every user. Any choice of* $\mathsf{K} = \theta(\mathsf{X}_a^n)$ *can therefore be recovered by every user without any discussion, satisfying the recoverability constraint* (4) *trivially. Since there is no public discussion required, the secrecy constraint* (5) *also holds immediately by taking a portion of the bits from* X_a^n *to be the key bits in* K. *Finally, setting* $\tilde{\mathsf{Z}}_i = \zeta_i(\mathsf{X}_a^n) = \theta(\mathsf{X}_a^n)$ *for all* $i \in V$ *ensures* $H(\tilde{\mathsf{Z}}_V) \leq H(\mathsf{K})$, *satisfying the entropy limit* (7) *with* α *equal to the key rate. Hence,* $\tilde{C}_{\mathsf{S}}(\alpha) \geq \alpha$, *as desired. Indeed, we will show (by Proposition 5) that the reverse inequality holds in general, and so we have equality for* $\alpha \in [0,1]$ *for this example.*

For $\alpha = H(\mathsf{Z}_V) = H(\mathsf{X}_a, \mathsf{X}_b, \mathsf{X}_c) = 3$, *every user can simply retain their source without compression; that is, with* $\tilde{\mathsf{Z}}_i = \mathsf{Z}_i$ *for* $i \in V$ *while satisfying the entropy limit* (7). *Now, with* $\mathsf{K} = (\mathsf{X}_a^n, \mathsf{X}_b^n)$ *and* $\mathsf{F} = \mathsf{F}_2 = \mathsf{X}_b^n \oplus \mathsf{X}_c^n$ *where* $\oplus$ *is the elementwise XOR, it can be shown that both the recoverability* (4) *and secrecy* (5) *constraints hold. This is because user* 3 *can recover* X_b *from the XOR* $\mathsf{X}_b \oplus \mathsf{X}_c$ *with the side information* X_c. *Furthermore, the XOR bit is independent of* $(\mathsf{X}_a, \mathsf{X}_b)$ *and therefore does not leak any information about the key bits. With this scheme,* $\tilde{C}_{\mathsf{S}}(3) \geq 2$. *By the usual time-sharing argument, we have*

$$\tilde{C}_{\mathsf{S}}(\alpha) \geq \begin{cases} \frac{1+\alpha}{2} & \text{for } \alpha \in [1,3] \\ 2 & \text{for } \alpha \geq 3. \end{cases} \tag{16b}$$

Indeed, the reverse inequality can be argued using one of the main results (Theorem 1) and so the minimum admissible joint entropy will turn out to be $\alpha_{\mathsf{S}} = 3$.

3. Preliminaries

In this section, a brief summary of related results for the secrecy capacity and communication complexity will be given. The results for the two-user case are introduced first, followed by the more general results for the multi-user case, and the stronger results for the special hypergraphical source model. An example will also be given at the end to illustrate some of the results.

3.1. Two-User Case

As mentioned in the introduction, no single-letter characterization is known for $C_{\mathsf{S}}(R)$ and $\tilde{C}_{\mathsf{S}}(\alpha)$, even in the two-user case where $V := \{1,2\}$. Furthermore, while multi-letter characterizations for R_{S} and $C_{\mathsf{S}}(R)$ were given in [11] and [13], respectively, in the two-user case under interactive discussion, no such multi-letter characterization is known for the case with non-interactive discussion. Nevertheless, if one-way discussion from user 1 is considered, then the result of [7] (Theorem 2.4) and its extension [8] to continuous sources gave the following characterization of $C_{\mathsf{S}}(R)$:

$$C_{\mathsf{S},1}(R) := \sup I(\mathsf{Z}_1' \wedge \mathsf{Z}_2) \quad \text{where} \tag{17a}$$

$$I(\mathsf{Z}_1' \wedge \mathsf{Z}_1) - I(\mathsf{Z}_1' \wedge \mathsf{Z}_2) \leq R \tag{17b}$$

$$I(\mathsf{Z}_1' \wedge \mathsf{Z}_2 | \mathsf{Z}_1) = 0. \tag{17c}$$

The last constraint (17c) corresponds to the Markov chain $\mathsf{Z}_1' - \mathsf{Z}_1 - \mathsf{Z}_2$ and so the supremum is taken over the choices of the conditional distribution $P_{\mathsf{Z}_1'|\mathsf{Z}_1} = P_{\mathsf{Z}_1'|\mathsf{Z}_1,\mathsf{Z}_2}$. Using the double Markov

property as in [11], it follows that $C_S(0)$ can be characterized more explicitly by the Gács–Körner common information

$$J_{GK}(Z_1 \wedge Z_2) := \sup\{H(U) \mid H(U|Z_1) = H(U|Z_2) = 0\} \tag{18}$$

where U is a discrete random variable. If (18) is finite, a unique optimal solution U exists and is called the *maximum common function* of Z_1 and Z_2 because any common function of Z_1 and Z_2 must be a function of U. The communication complexity also has a more explicit characterization [11] (Equation (44))

$$R_{S,1} = J_{W,1}(Z_1 \wedge Z_2) - I(Z_1 \wedge Z_2) \quad \text{where} \tag{19}$$

$$J_{W,1}(Z_1 \wedge Z_2) := \inf\{H(W) \mid H(W|Z_1) = 0, I(Z_1 \wedge Z_2|W) = 0\} \tag{20}$$

and W is a discrete random variable. If $J_{W,1}(Z_1 \wedge Z_2)$ is finite, a unique optimal solution W exists and is called the *minimum sufficient statistics* of Z_1 for Z_2 since Z_2 can only depend on Z_1 through W.

In Section 4, the expression $C_{S,1}(R)$ will be related to the compressed secret key agreement restricted to the two-user case when the entropy limit is imposed only on user 1. This duality relationship in the two-user case will serve as the motivation of the main results for the multi-user case. Indeed, the desired characterization of $\tilde{C}_S(\alpha)$ for the two-user case has appeared in [30] (Lemma 4.1) for the scalar Gaussian source model:

$$\tilde{C}_{S,1}(\alpha) := \sup I(Z_1' \wedge Z_2) \quad \text{where} \tag{21a}$$

$$I(Z_1' \wedge Z_1) \le \alpha \tag{21b}$$

$$I(Z_1' \wedge Z_2|Z_1) = 0. \tag{21c}$$

For the general source model, the expression (21) has also appeared before with other information-theoretic interpretations, as mentioned in [43]. In particular, the Lagrangian dual of (21) reduces to the dimension reduction technique called the information bottleneck method in [39], where Z_1 is an observable used to predict the target Z_2, and Z_1' is a feature of Z_1 that captures as much mutual information with the target variable as possible per bit of mutual information with the observable. Interestingly, the principal of the information bottleneck method was also proposed in [44,45] as a way to understand deep learning, since the best prediction of Z_2 from Z_1 is nothing but a particular feature of Z_1 sharing a lot of mutual information with Z_2.

3.2. General Source with Finite Alphabet Set

Consider the multi-user case where $|V| \ge 2$. If Z_V takes values from a finite set, then the unconstrained secrecy capacity was shown in [6] to be achievable via *communication for omniscience (CO)* and equal to

$$C_S(\infty) = H(Z_V) - R_{CO}, \tag{22}$$

where R_{CO} is the smallest rate of CO [6] characterized by the linear program

$$R_{CO} = \min_{r_V} r(V) \quad \text{such that} \tag{23a}$$

$$r(B) \ge H(Z_B|Z_{V\setminus B}) \quad \forall B \subsetneq V, \tag{23b}$$

where $r(B)$ denotes the sum $\sum_{i\in B} r_i$. Further, R_{CO} can be achieved by non-interactive discussion. It follows that

$$R_S \le R_{CO}, \quad \text{or equivalently} \tag{24a}$$

$$C_S(R) = C_S(\infty) \quad R \ge R_{CO}. \tag{24b}$$

It was also pointed out in [6] that private randomization does not increase $C_S(\infty)$. Hence, if Z_V is finite, we have

$$\alpha_S \leq H(\mathsf{Z}_V) \tag{25}$$

because $C_S(\infty)$ can be achieved with $\tilde{\mathsf{Z}}_i = \mathsf{Z}_i$. While it seems plausible that randomization does not decrease R_S nor increase $C_S(R)$ for any $R \geq 0$, a rigorous proof remains elusive. Similarly, it appears plausible that neither α_S nor $\tilde{C}_S(\alpha)$ are affected by randomization, but, again, no proof is known yet.

An alternative characterization of $C_S(\infty)$ was established in [24,33] by showing that the divergence bound in [6] is tight in the case without helpers. More precisely, with $\Pi'(V)$ defined as the set of partitions of V into at least two non-empty disjoint sets, then

$$C_S(\infty) = I(\mathsf{Z}_V) := \min_{\mathcal{P}\in\Pi'(V)} I_{\mathcal{P}}(\mathsf{Z}_V), \quad \text{where} \tag{26a}$$

$$\begin{aligned} I_{\mathcal{P}}(\mathsf{Z}_V) &:= \frac{1}{|\mathcal{P}|-1} D\left(P_{\mathsf{Z}_V} \,\middle\|\, \prod_{C\in\mathcal{P}} P_{\mathsf{Z}_C}\right) \\ &= \frac{1}{|\mathcal{P}|-1}\left[\sum_{C\in\mathcal{P}} H(\mathsf{Z}_C) - H(\mathsf{Z}_V)\right]. \end{aligned} \tag{26b}$$

In the bivariate case for which $V = \{1,2\}$, $I(\mathsf{Z}_V)$ reduces to Shannon's mutual information $I(\mathsf{Z}_1 \wedge \mathsf{Z}_2)$. It was further pointed out in [32] that $I(\mathsf{Z}_V)$ is the minimum solution γ to the *residual independence relation*

$$H(\mathsf{Z}_V) - \gamma = \sum_{C\in\mathcal{P}} [H(\mathsf{Z}_C) - \gamma] \tag{27}$$

for some $\mathcal{P} \in \Pi'(V)$. To get an intuition of the above relation, notice that $\gamma = 0$ is a solution when the joint entropy $H(\mathsf{Z}_V)$ on the left is equal to the sum of entropies $H(\mathsf{Z}_C)$'s on the right for some partition $\mathcal{P}$. In other words, the MMI is the smallest value of γ removal of which leads to an independence relation; i.e., the total residual randomness on the left is equal to the sum of individual residual randomness on the right according to some partitioning of the random variables. It was further shown in [32] that there is a unique finest optimal partition to (26a) with a clustering interpretation in [36]. The MMI is also computable in polynomial time, following the result of Fujishige [46].

In the opposite extreme with $R \to 0$, it is easy to argue that

$$C_S(0) \geq J_{GK}(\mathsf{Z}_V) \tag{28}$$

where $J_{GK}(\mathsf{Z}_V)$ is the multivariate extension of the Gács–Körner common information in (18)

$$J_{GK}(\mathsf{Z}_V) := \sup\{H(\mathsf{U}) \mid H(\mathsf{U}|\mathsf{Z}_i) = 0 \ \forall i \in V\} \tag{29}$$

with U again chosen as a discrete random variable. Note that even without any public discussion, every user can compress their source independently to U^n where U is the maximum common function if $J_{GK}(\mathsf{Z}_V)$ is finite. Hence, it is easy to achieve a secret key rate of $H(\mathsf{U}) = J_{GK}(\mathsf{Z}_V)$ without any discussion. The reverse inequality of (28) seems plausible, but has not yet been proven, except in the two-user case. The technique in [7] which relies on the Csiszár sum identity does not appear to extend to the multi-user case to give a matching converse.

3.3. Hypergraphical Sources

Stronger results have been derived for the following special source model:

Definition 3 (Definition 2.4 of [24]). 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 edge variables* X_e *for* $e \in E$ *with* $H(\mathsf{X}_e) > 0$,

$$\mathsf{Z}_i := (\mathsf{X}_e \mid e \in E, i \in \xi(e)) \quad \text{, for } i \in V. \tag{30}$$

In the special case for which the hypergraph is a graph (i.e., $|\xi(e)| = 2$*), the model reduces to the pairwise independent network (PIN) model in [23]. The hypergrahical source can also be viewed as a special case of the finite linear source considered in [47] if the edge random variables take values from a finite field.*

For hypergraphical sources, various bounds on R_{S} and $C_{\mathrm{S}}(R)$ have been derived in [20–22,26]. The achieving scheme makes use of the idea of decremental secret key agreement [28,29], where the redundant or less useful edge variables are removed or reduced before public discussion. This is a special case of the compressed secret key agreement, where the compression step simply selects the more useful edge variables up to the joint entropy limit.

For the PIN model, it turns out that decremental secret key agreement is optimal, leading to a single-letter characterization of R_{S} and $C_{\mathrm{S}}(R)$ in [26]:

$$R_{\mathrm{S}} = (|V| - 2) C_{\mathrm{S}}(\infty). \tag{31a}$$

$$C_{\mathrm{S}}(R) = \min\left\{ \frac{R}{|V| - 2}, C_{\mathrm{S}}(\infty) \right\} \quad \text{for } R \geq 0. \tag{31b}$$

It can be verified that (31a) is the smallest value of R such that $C_{\mathrm{S}}(R) = C_{\mathrm{S}}(\infty)$ using (31b). While the proof of the converse (i.e., $\leq$ for (31b)) is rather involved, the achievability is by a simple tree packing protocol, which belongs to the decremental secret key agreement approach that removes excess edges unused for the maximum tree packing. In other words, the achieving scheme is a compressed secret key agreement scheme. This connection will lead to a single-letter characterization of $\tilde{C}_{\mathrm{S}}(\alpha)$ for the PIN model (in Theorem 2).

To illustrate the above results, a single-letter characterization for $C_{\mathrm{S}}(R)$ is derived in the following for the source in Example 1. It also demonstrates how an exact characterization for $C_{\mathrm{S}}(R)$ can be extended from a PIN model to a hypergraphical model via some contrived arguments. The characterization is also useful later in Example 3 to give an exact characterization of $\tilde{C}_{\mathrm{S}}(\alpha)$.

Example 2. *The source defined in* (15) *in Example 1, for instance, is a hypergraphical source with* $E = \{a, b, c\}$, $\xi(a) = \{1, 2, 3\}$, $\xi(b) = \{1, 2\}$ *and* $\xi(c) = \{2, 3\}$. *By* (23), *we have* $R_{\mathrm{CO}} = 1$ *with the optimal solution* $r_1 = r_3 = 0$ *and* $r_2 = 1$. *This means that user* 2 *needs to discuss* 1 *bit to attain omniscience. In particular, user* 2 *can reveal the XOR* $\mathsf{X}_b \oplus \mathsf{X}_c$ *so that users* 1 *and* 3 *can recover* X_c *and* X_b, *respectively, from their observations. By* (24b), *we have*

$$C_{\mathrm{S}}(R) = C_{\mathrm{S}}(\infty) = H(\mathsf{Z}_V) - R_{\mathrm{CO}} = 2 \quad \text{for } R \geq R_{\mathrm{CO}} = 1. \tag{32}$$

It can also be checked that the alternative characterization of $C_{\mathrm{S}}(\infty)$ *in* (26) *gives*

$$C_{\mathrm{S}}(\infty) = I(\mathsf{Z}_V) = \frac{1}{2}\left[H(\mathsf{Z}_1) + H(\mathsf{Z}_2) + H(\mathsf{Z}_3) - H(\mathsf{Z}_{\{1,2,3\}}) \right] = 2.$$

Next, we argue that

$$C_{\mathrm{S}}(R) = 1 + R \quad \text{for } R \in [0, 1]. \tag{33}$$

The achievability (i.e., the inequality $C_{\mathrm{S}}(R) \geq 1 + R$*) is by the usual time-sharing argument. In particular, the bound* $C_{\mathrm{S}}(0.5) \geq 1.5$, *for example, can be achieved by the compressed secret key agreement scheme in Example 1 with* $\alpha = 2$ *(i.e., by time-sharing the compressed secret key agreement schemes for* $\alpha = 1$ *and for* $\alpha = 3$ *equally). More precisely, we set* $\tilde{\mathsf{Z}}_1 = (\mathsf{X}_a^n, \mathsf{X}_b^{\lfloor n/2 \rfloor})$, $\tilde{\mathsf{Z}}_2 = (\mathsf{X}_a^n, \mathsf{X}_b^{\lfloor n/2 \rfloor}, \mathsf{X}_c^{\lfloor n/2 \rfloor})$, $\tilde{\mathsf{Z}}_3 = (\mathsf{X}_a^n, \mathsf{X}_c^{\lfloor n/2 \rfloor})$, $\mathsf{K} = (\mathsf{X}_a^n, \mathsf{X}_b^{\lfloor n/2 \rfloor})$, *and* $\mathsf{F} = \mathsf{F}_2 = \mathsf{X}_b^{\lfloor n/2 \rfloor} \oplus \mathsf{X}_c^{\lfloor n/2 \rfloor}$. *It follows that the public discussion rate is* $\limsup_{n \to \infty} \frac{1}{n} \log |F| = 0.5$.

Now, to prove the reverse inequality $\leq$ for (33), we modify the source Z_V to another source Z'_V defined as follows with an additional uniformly random and independent bit X_d:

$$\mathsf{Z}'_1 := (\mathsf{X}_a, \mathsf{X}_b), \quad \mathsf{Z}'_2 := (\mathsf{X}_a, \mathsf{X}_b, \mathsf{X}_c, \mathsf{X}_d), \quad \text{and} \quad \mathsf{Z}'_3 := (\mathsf{X}_c, \mathsf{X}_d).$$

Note that Z'_V is different from Z_V; namely, Z'_2 is obtained from Z_2 by adding X_d, and Z'_3 is obtained from Z_3 by adding X_d and removing X_a. It follows that Z'_V is a PIN. By (26) and (31b), the constrained secrecy capacity for the modified source Z'_V is

$$C'_{\mathsf{S}}(R) = \min\{R, 2\}.$$

The desired inequality is proved if we can show that

$$C'_{\mathsf{S}}(R+1) \geq C_{\mathsf{S}}(R).$$

To argue this, we note that, if user 2 reveals $\mathsf{F}'_2 = \mathsf{X}_a \oplus \mathsf{X}_d$ in public, then user 3 can recover X_a. Furthermore, F'_2 does not leak any information about X_a, and so the source Z'_V effectively emulates the source Z_V. Consequently, any optimal discussion scheme F_V that achieves $C_{\mathsf{S}}(R)$ for Z_V can be used to achieve the same secret key rate but after an additional bit of discussion F'_2. This gives the desired inequality that establishes (33).

4. Multi-Letter Characterization

We start with a simple multi-letter characterization of the compressed secrecy capacity in terms of the MMI (26).

Proposition 2. *For any $\alpha \geq 0$, we have*

$$\tilde{C}_{\mathsf{S}}(\alpha) = \sup \lim_{n\to\infty} \frac{1}{n} I(\tilde{\mathsf{Z}}_V) \tag{34}$$

where the supremum is over all valid compressed source $\tilde{\mathsf{Z}}_V$ satisfying the joint entropy limit (7).

Proof. This is because the compressed secrecy capacity is simply the secret key agreement on a compressed source. Hence, by (26), the MMI on the compressed source gives the compressed secrecy capacity. □

The characterization in (34) is simpler than the formulation in (6) because it does not involve the random variables F and K, nor the recoverability (4) and secrecy (5) constraints. Although such a multi-letter expression is not computable and therefore not accepted as a solution to the problem, it serves as an intermediate step that helps derive further results. More precisely, consider the bivariate case where $V = \{1, 2\}$. Then, (34) becomes

$$\tilde{C}_{\mathsf{S}}(\alpha) = \sup \lim_{n\to\infty} \frac{1}{n} I(\tilde{\mathsf{Z}}_1 \wedge \tilde{\mathsf{Z}}_2) \quad \text{where} \tag{35a}$$

$$\limsup_{n\to\infty} \frac{1}{n} H(\tilde{\mathsf{Z}}_1, \tilde{\mathsf{Z}}_2) - \alpha \leq 0. \tag{35b}$$

If in addition the joint entropy constraint (35b) is replaced by the entropy constraint on user 1 only, i.e.,

$$\limsup_{n\to\infty} \frac{1}{n} H(\tilde{\mathsf{Z}}_1) - \alpha \leq 0, \tag{35c}$$

then $\tilde{C}_{\mathsf{S}}(\alpha)$ can be single-letterized by standard techniques as in [7] to $\tilde{C}_{\mathsf{S},1}(\alpha)$ defined in (21). The following gives a simple upper bound that is tight for sufficiently small α.

Proposition 3. *$\tilde{C}_{S,1}(\alpha)$ defined in (21) is continuous, non-decreasing, and concave in $\alpha \geq 0$ with*

$$\tilde{C}_{S,1}(\alpha) \leq \alpha. \tag{36}$$

Furthermore, equality holds iff $\alpha \leq J_{GK}(Z_1 \wedge Z_2)$.

Proof. Monotonicity is obvious. Continuity and concavity can be shown by the usual time-sharing argument as in Proposition 1. (36) follows directly from the data processing inequality that $I(Z_1' \wedge Z_2) \leq I(Z_1' \wedge Z_1)$ under the Markov chain $Z_1' - Z_1 - Z_2$ required in (21c). If $\alpha \leq J_{GK}(Z_1 \wedge Z_2)$, then there exists a feasible solution U to (18) (a common function of Z_1 and Z_2) with $H(U) \geq \alpha$, and so the compressed sources $\tilde{Z}_1$ and $\tilde{Z}_2$ can be chosen as a function of U^n to achieve the equality for (36). Conversely, suppose $J_{GK}(Z_1 \wedge Z_2)$ is finite and (36) is satisfied with equality. Then, in addition to $Z_1' - Z_1 - Z_2$, we also have $Z_1' - Z_2 - Z_1$, which implies by the double Markov property that for the maximum common function U achieving $J_{GK}(Z_1 \wedge Z_2)$ defined in (18),

$$I(Z_1' \wedge Z_1, Z_2|U) = 0 \quad (\text{or } Z_1' - U - (Z_1, Z_2)).$$

In other words, the optimal Z_1' is a stochastic function of the maximum common function of Z_1 and Z_2, and so $\alpha = I(Z_1' \wedge Z_2) \leq J_{GK}(Z_1 \wedge Z_2)$ as desired. □

We will show that the above upper bound in (36) extends to the multi-user case (in Proposition 5). However, for $\alpha \geq J_{GK}(Z_1 \wedge Z_2)$, the above upper bound is not tight even in the two-user case. To improve the upper bound, the following duality between $\tilde{C}_{S,1}$ and $C_{S,1}$ will be used and extended to the multi-user case (in Theorem 1).

Proposition 4. *For $\alpha \geq J_{GK}(Z_1 \wedge Z_2)$,*

$$\tilde{C}_{S,1}(\alpha) = C_{S,1}(\alpha - \tilde{C}_{S,1}(\alpha)). \tag{37}$$

Furthermore, the set of optimal solutions to the left (achieving $\tilde{C}_{S,1}(\alpha)$ defined in (21)) is the same as the set of optimal solutions to the right (achieving $C_{S,1}(R)$ in (17) with $R = \alpha - \tilde{C}_{S,1}(\alpha)$). It follows that the minimum admissible entropy (12) but with the entropy constraint on user 1 instead is

$$\alpha_{S,1} = R_{S,1} + I(Z_1 \wedge Z_2) = J_{W,1}(Z_1 \wedge Z_2) \tag{38}$$

where $R_{S,1}$ and $J_{W,1}(Z_1 \wedge Z_2)$ are defined in (19) and (20), respectively.

Proof. Set $R = \alpha - \tilde{C}_{S,1}(\alpha)$. Consider first an optimal solution Z_1' to $\tilde{C}_{S,1}(\alpha)$ and show that it is also an optimal solution to $C_{S,1}(R)$. By optimality,

$$I(Z_1' \wedge Z_2) = \tilde{C}_{S,1}(\alpha). \tag{39}$$

By the constraint (21b), $I(Z_1' \wedge Z_1) \leq \alpha$. It follows that the constraint (17b) holds, and so Z_1' is a feasible solution to $C_{S,1}(R)$; i.e., we have $\geq$ for (37) that

$$\tilde{C}_{S,1}(\alpha) \geq C_{S,1}(\alpha - \tilde{C}_{S,1}(\alpha)). \tag{40}$$

To show that Z_1' is also optimal to $C_{S,1}(R)$, suppose to the contrary that there exists a strictly better solution Z_1'' to $C_{S,1}(R)$; i.e., with

$$I(Z_1'' \wedge Z_2) > I(Z_1' \wedge Z_2) = \tilde{C}_{S,1}(\alpha). \tag{41}$$

It follows that

$$I(\mathsf{Z}_1'' \wedge \mathsf{Z}_1) > I(\mathsf{Z}' \wedge \mathsf{Z}_1) = \alpha. \tag{42}$$

The last equality means that the constraint (21b) is satisfied with equality. If on the contrary that the equality does not hold, setting Z_1' to be Z_1'' for some fraction $\lambda > 0$ of time gives a better solution to $C_{\mathsf{S},1}(R)$, contradicting the optimality of Z_1'. The first inequality can also be argued similarly by the optimality of Z_1'. Now, we have

$$\frac{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_2) - I(\mathsf{Z}_1' \wedge \mathsf{Z}_2)}{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_1) - I(\mathsf{Z}_1' \wedge \mathsf{Z}_1)} \overset{\text{(a)}}{\leq} \frac{I(\mathsf{Z}_1' \wedge \mathsf{Z}_2)}{I(\mathsf{Z}_1' \wedge \mathsf{Z}_1)} \overset{\text{(b)}}{\leq} 1,$$

where (a) is by the concavity of $\tilde{C}_{\mathsf{S},1}(\alpha)$; and (b) is by the upper bound $\tilde{C}_{\mathsf{S},1}(\alpha) \leq \alpha$ in (36). We note that equality cannot hold simultaneously for (a) and (b) because, otherwise, we have $\frac{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_2)}{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_1)} = 1$, which, together with (41) and (42), contradicts the result in Proposition 3 that $\tilde{C}_{\mathsf{S},1}(\alpha) < \alpha$ (with strict inequality) for $\alpha > J_{\mathrm{GK}}(\mathsf{Z}_1 \wedge \mathsf{Z}_2)$. Hence,

$$\frac{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_2) - I(\mathsf{Z}_1' \wedge \mathsf{Z}_2)}{I(\mathsf{Z}_1'' \wedge \mathsf{Z}_1) - I(\mathsf{Z}_1' \wedge \mathsf{Z}_1)} < 1,$$

which, together with (41) and (42), implies

$$I(\mathsf{Z}_1'' \wedge \mathsf{Z}_1) - I(\mathsf{Z}_1'' \wedge \mathsf{Z}_2) > \alpha - \tilde{C}_{\mathsf{S},1}(\alpha) = R$$

contradicting even the feasibility of Z_1'' to $C_{\mathsf{S},1}(R)$; namely, the constraint (17b) with Z_1' replaced with Z_1''. This completes the proof of the optimality of Z_1' to $C_{\mathsf{S},1}(R)$.

Next, consider showing that an optimal solution Z_1' to $C_{\mathsf{S},1}(R)$ is also optimal to $\tilde{C}_{\mathsf{S},1}(\alpha)$. Then,

$$I(\mathsf{Z}_1' \wedge \mathsf{Z}_1) \leq R + I(\mathsf{Z}_1' \wedge \mathsf{Z}_2) = \alpha - \tilde{C}_{\mathsf{S},1}(\alpha) + C_{\mathsf{S},1}(R) \leq \alpha$$

where the first inequality is by (17b); the second equality is by the optimality of Z_1'; and the last inequality follows from (40). Hence, the constraint (21b) holds and so Z_1' is a feasible solution for $\tilde{C}_{\mathsf{S},1}(\alpha)$. If on the contrary that we have a better solution Z_1'' for $\tilde{C}_{\mathsf{S},1}(\alpha)$, then Z_1'' can be shown to be a feasible solution for $C_{\mathsf{S},1}(R)$, contradicting the optimality of Z_1'. □

5. Main Results

The following extends the single-letter upper bound (36) in Proposition 3 to the multi-user case.

Proposition 5. *$\tilde{C}_{\mathsf{S}}(\alpha) \leq \alpha$ with equality if $\alpha \leq J_{\mathrm{GK}}(\mathsf{Z}_V)$.*

Proof. The upper bound $\tilde{C}_{\mathsf{S}}(\alpha) \leq \alpha$ is because $n\tilde{C}_{\mathsf{S}}(\alpha)$ cannot exceed the unconstrained secrecy capacity for the compressed source $\tilde{\mathsf{Z}}_V$, which, by (22) and (7), is upper-bounded by $H(\tilde{\mathsf{Z}}_V) \leq n\,[\alpha + \delta_n]$ for some $\delta_n \to 0$ as $n \to \infty$.

Next, to prove the equality condition is sufficient, suppose $\alpha \leq J_{\mathrm{GK}}(\mathsf{Z}_V)$. Then, each user can compress their source directly to a common secret key at rate α without any public discussion. Hence, $\tilde{C}_{\mathsf{S}}(\alpha) = \alpha$ as desired. □

Note that unlike the two-user case in Proposition 3, the equality condition above in terms of the multivariate Gács–Körner common information is sufficient but not shown to be necessary. Nevertheless, necessity seems very plausible, as there seems to be no counter-example that suggests otherwise.

As in Proposition 4, a duality can be proved in the multi-user case, relating the compressed secret key agreement problem to the constrained secrecy key agreement problem.

Theorem 1. *With $C_S(R)$ and R_S defined in (9) and (12) respectively, we have*

$$\alpha_S \geq R_S + C_S(\infty) \tag{43a}$$
$$\tilde{C}_S(\alpha) \leq C_S(\alpha - \tilde{C}_S(\alpha)) \tag{43b}$$

for all $\alpha \geq 0$.

Proof. Equation (43a) can be obtained from (43b) by setting $\alpha = \alpha_S$ as follows:

$$C_S(\infty) \overset{(a)}{\geq} C_S(\alpha_S - \tilde{C}_S(\alpha_S)) \overset{(b)}{\geq} \tilde{C}_S(\alpha_S) \overset{(c)}{=} C_S(\infty)$$

where (b) is given by (43b) with $\alpha = \alpha_S$; while (a) and (c) follows directly from (11), (13), and monotonicity. It follows that the inequalities (a) and (b) hold with equality. In particular, equality for (a) means that $C_S(R) = C_S(\infty)$ for $R \geq \alpha_S - \tilde{C}_S(\alpha_S) = \alpha_S - C_S(\infty)$, implying (43a) as desired.

To show (43b), we consider an optimal compressed secret key agreement scheme achieving $\tilde{C}_S(\alpha)$ with an arbitrary entropy limit α. It suffices to show that the discussion rate need not be larger than $\alpha - \tilde{C}_S(\alpha)$. Letting $\tilde{Z}_V$ be the optimal compressed source and $\tilde{R}_{CO}$ be the smallest rate of communication for omniscience of $\tilde{Z}_V$, which is given by (23) with Z_V replaced by $\tilde{Z}_V$, the discussion rate for the omniscience strategy is

$$\frac{1}{n}\tilde{R}_{CO} = \frac{1}{n}\left[H(\tilde{Z}_V) - I(\tilde{Z}_V)\right]$$

by (22). This simplifies to $\alpha - \tilde{C}_S(\alpha)$ as desired in the limit $n \to \infty$. Note that since the omniscience strategy is non-interactive, the desired hold even if C_S and R_S are defined with non-interactive discussion. □

While it is obvious from the above proof that a compressed secret key agreement scheme can be used as a constrained secret key agreement scheme, yielding one of the best lower bounds for $C_S(R)$ in [26], the above result also means that a converse result for constrained secret key agreement can be applied to compressed secret key agreement. Upper bounds on $\tilde{C}_S(\alpha)$ may be obtained from the upper bounds for $C_S(R)$ such as those in [26]. It turns out that this approach can give better upper bounds which, surprisingly, are tight for the PIN model as mentioned in Section 3.3. This leads to the following exact single-letter characterization of $\tilde{C}_S(\alpha)$.

Theorem 2. *For the PIN model in Definition 3,*

$$\alpha_S = (|V| - 1)C_S(\infty) \tag{44a}$$
$$\tilde{C}_S(\alpha) = \min\left\{\frac{\alpha}{|V| - 1}, C_S(\infty)\right\} \tag{44b}$$

for all $\alpha \geq 0$.

Proof. Equation (44a) follows easily from (44b) by setting the two terms in the minimization to be equal and solving for α. To show (44b), note that by (31b) we have

$$C_S^{-1}(\gamma) = (|V| - 2)\gamma \quad \forall \gamma < C_S(\infty)$$

because $C_S(R)$ is non-decreasing and concave, and thus it must be strictly non-decreasing before it reaches $C_S(\infty) = C_S(\infty)$. Now, by (43b),

$$\begin{aligned}\alpha - \tilde{C}_S(\alpha) &\geq C_S^{-1}(\tilde{C}_S(\alpha)) \\ &= (|V| - 2)\tilde{C}_S(\alpha)\end{aligned}$$

for any $\alpha \geq 0$ such that $\tilde{C}_S(\alpha) < C_S(\infty)$; that is, for $\alpha \leq \alpha_S$, and thus $\tilde{C}_S(\alpha) \leq \frac{\alpha}{|V|-1}$. This implies $\leq$ for (44b). The bound is achievable by the same achieving scheme as in [26] (Theorem 4.4) along the idea of decremental secrecy key agreement and the tree packing protocol in [27]. More precisely, every $(|V|-1)$ bits of edge variable forming a spanning tree are turned into a secret key bit by the tree packing protocol. This results in the factor of $(|V|-1)$ in (44), which corresponds to the number of edges in a spanning tree. □

For the more general source model, the idea of decremental secret key agreement needs to be refined, because there need not be any edge variables to remove. The following is a simple extension that leads to a single-letter lower bound on $\tilde{C}_S(\alpha)$.

Theorem 3. *A single-letter lower bound on* $\tilde{C}_S(\alpha)$ *is*

$$\tilde{C}_S(\alpha) \geq I(Z'_V|Q) \tag{45}$$

for any random vector (Q, Z'_V) *taking values from a finite set and satisfying*

$$I(Q \wedge Z_V) = 0 \tag{46a}$$
$$H(Z'_i|Z_i, Q) = 0 \quad \forall i \in V \tag{46b}$$
$$H(Z'_V|Q) \leq \alpha. \tag{46c}$$

Furthermore, it is admissible to have $|Q| \leq 3$.

Proof. By (46b), we have $Z'_i = \xi_i(Z_i, Q)$ for some function ξ_i. W.l.o.g., we let $Q := \{1, \ldots, k\}$ for some integer $k > 0$. We choose $\tilde{Z}_i$ to be the following function of Z_i^n:

$$\tilde{Z}_i = ((\xi_i(Z_{i\tau}, q) \mid n_{q-1} < \tau \leq n_q) \mid 1 \leq q \leq k) \quad \text{where}$$
$$n_0 = 0 \quad \text{and} \quad n_q = \left\lfloor n \sum_{j=1}^{q} P_Q(j) \right\rfloor \quad \text{for } 1 \leq q \leq k.$$

Essentially, Q acts as a time-sharing random variable, where $P_Q(q)$ is the fraction of time the source Z_i is processed to $Z_i^{(q)} := \xi_i(Z_i, q)$, for $1 \leq q \leq k$. More precisely, we have that $\frac{n_q - n_{q-1}}{n}$ converges to $P_Q(q)$, and thus

$$\frac{1}{n} I(\tilde{Z}_V) = \sum_{q=1}^{k} I(Z_V^{(q)}) \frac{n_q - n_{q-1}}{n}$$
$$\xrightarrow{n\to\infty} I(Z'_V|Q).$$

Similarly,

$$\frac{1}{n} H(\tilde{Z}_V) \xrightarrow{n\to\infty} H(Z'_V|Q) \leq \alpha$$

by (46c), satisfying the entropy limit of (7). Hence, $\tilde{Z}_V$ is a valid compressed source, the unconstrained capacity of which is $I(Z'_V|Q)$, leading to the desired lower bound of (45).

The condition that $|Q| \leq 3$ is admissible follows from the usual argument by the well-known Eggleston–Carathéodory theorem. More precisely, by letting

$$\mathscr{S} := \{(I(Z'_V|Q = q), H(Z'_V|Q = q)) \mid P_{Z_V|Q=q} = P_{Z_V},$$
$$H(Z'_i|Z_i, Q = q) = 0\}.$$

It can be seen that the conditions above are equivalent to (46a) and (46b), respectively, and thus the set of feasible values to (46), namely

$$(I(\mathsf{Z}'_V|\mathsf{Q}), H(\mathsf{Z}'_V|\mathsf{Q})) = \sum_{q\in Q} P_{\mathsf{Q}}(q)(I(\mathsf{Z}_V^q), H(\mathsf{Z}_V^q)),$$

is equal to the convex hull of $\mathscr{S}$. Because the dimension of $\mathscr{S}$ is at most 2, the pair $(\tilde{C}_{\mathsf{S}}(\mathsf{Z}_V), \alpha)$ can be obtained as a convex combination of at most three points in $\mathscr{S}$ as desired by the Eggleston–Carathéodory theorem. □

The main results above can be illustrated as follows using the hypergraphical source in Example 1 given earlier. In particular, an exact single-letter characterization of $\tilde{C}_{\mathsf{S}}(\alpha)$ will be derived, even though such an exact characterization is not known for general hypergraphical sources.

Example 3. *Consider the source defined in* (15) *in Example 1. It is shown that* (16a) *and* (16b) *are satisfied with equality, which gives the desired single-letter characterization of* $\tilde{C}_{\mathsf{S}}(\alpha)$.

It is easy to show that $J_{\mathrm{GK}}(\mathsf{Z}_V) = 1$ *as* X_a *is the maximum common function of* Z_1, Z_2, *and* Z_3. *Hence, the reverse inequality of* (16a) *follows from Proposition 5.*

The reverse inequality for (16b) *can be argued using the bound in Theorem 1 by* $C_{\mathsf{S}}(R)$ *and the characterization of* $C_{\mathsf{S}}(R)$ *in Example 2. More precisely, by* (32), *the unconstrained secrecy capacity* $C_{\mathsf{S}}(\infty) = 2$. *Then, by* (33), *we have* $C_{\mathsf{S}}^{-1}(\gamma) \le \gamma - 1$ *for all* $\gamma \le C_{\mathsf{S}}(\infty) = 2$. *Now, by* (43b),

$$\alpha - \tilde{C}_{\mathsf{S}}(\alpha) \le C_{\mathsf{S}}^{-1}(\tilde{C}_{\mathsf{S}}(\alpha)) \le \tilde{C}_{\mathsf{S}}(\alpha) - 1$$

and thus $\tilde{C}_{\mathsf{S}}(\alpha) \le \frac{1+\alpha}{2}$ *for* $\tilde{C}_{\mathsf{S}}(\alpha) \le 2$. *This completes the proof.*

6. Conclusion and Extensions

Inspired by the idea of decremental secret key agreement and its application to the constrained secret key agreement problem, we have formulated a multiterminal secret key agreement problem with a more general source compression step that applies beyond the hypergraphical source model. This formulation allows us to separate and compare the issues of source compression and discussion rate constraint in secret key agreement. While a single-letter characterization of the compressed secrecy capacity and admissible entropy limit remains unknown, single-letter bounds have been derived and they are likely to be tight for the hypergraphical model, and possibly more general source models such as the finite linear source model [47]. For the PIN model in particular, the bounds are tight, giving rise to a complete characterization of the capacity in Theorem 2. One way to improve the current converse results is to show whether the equality condition in Proposition 5 is necessary; that is, $\tilde{C}_{\mathsf{S}}(\alpha) < \alpha$ for $\alpha > J_{GK}(\mathsf{Z}_V)$. By the duality in Theorem 1, the condition is necessary if one can show that $C_{\mathsf{S}}(0) = J_{\mathrm{GK}}(\mathsf{Z}_V)$; i.e., (28) holds with equality. Such equality can be proved for hypergraphical as well as finite linear sources by extending the lamination techniques in [26]. It is hopeful that a complete solution can be given for the finite linear source model and the well-known jointly Gaussian source model. The bounds (43) in the duality result may plausibly be tight for these special sources, in which case non-interactive discussion suffices to achieve the constrained secrecy capacity. The current achievability results may also be improved. In particular, for the two-user case with joint entropy constraint (35), the lower bound in (45) can be improved to $\tilde{C}_{\mathsf{S}}(\alpha) \ge \max I(\mathsf{Z}'_1 \wedge \mathsf{Z}'_2)$ where $I(\mathsf{Z}'_1 \wedge \mathsf{Z}_1) + I(\mathsf{Z}'_2 \wedge \mathsf{Z}_2) \le \alpha$ and $\mathsf{Z}'_1 - \mathsf{Z}_1 - \mathsf{Z}_2 - \mathsf{Z}'_2$. Whether this improvement is strict or is the best possible is not yet clear, but an extension to the multi-user case seems possible. A related open problem is to characterize the $C_{\mathsf{S}}(R)$ in the two-user case with two-way non-interactive discussion. A simpler question is whether two-way non-interactive discussion can be strictly better than one-way discussion.

As pointed out before, by regarding the secrecy capacity as a measure of mutual information, an optimal source compression scheme translates to a dimension reduction technique which is potentially useful for machine learning. A closely related line of work is the study of the strong data processing

inequality in [43,48,49]; in particular, the ratio $s^*(\mathsf{Z}_1;\mathsf{Z}_2) := \sup \frac{I(\mathsf{Z}_1' \wedge \mathsf{Z}_2)}{I(\mathsf{Z}_1' \wedge \mathsf{Z}_1)}$ where—as in (21)—the supremum is taken over the choice of the conditional distribution $P_{\mathsf{Z}_1'|\mathsf{Z}_1,\mathsf{Z}_2}$ such that $\mathsf{Z}_1' - \mathsf{Z}_1 - \mathsf{Z}_2$ forms a Markov chain and $I(\mathsf{Z}_1' \wedge \mathsf{Z}) > 0$. It is straightforward to show that $\sup_{\alpha \geq 0} \frac{\tilde{C}_S(\alpha)}{\alpha}$ for the two-user case in (35) is upper bounded by $s^*(\mathsf{Z}_1;\mathsf{Z}_2)$ and $s^*(\mathsf{Z}_2;\mathsf{Z}_1)$. However, a sharper bound and a more precise mathematical connection may be possible, and the result may be extended to the multivariate case. Furthermore, the linearization considered in [50] may potentially be adopted to provide a single-letter lower bound on the compressed secrecy capacity. As in [13,48], the problem may also be related to a notion of maximum correlation appropriately extended to the multivariate case.

Acknowledgments: The work of Chung Chan was supported in part by the Vice-Chancellor's One-off Discretionary Fund of The Chinese University of Hong Kong under Project VCF2014030 and Project VCF2015007 and in part by the University Grants Committee of the Hong Kong Special Administrative Region, China, under Project 14200714. The author would like to thank Ali Al-Bashabsheh for pointing out a mistake in an earlier proof and Qiaoqiao Zhou for the discussion of the two-user case. The author would also like to thank Shao-Lun Huang, Navin Kashyap, and Manuj Mukherjee for their valuable comments and pointers to related work.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Maurer, U.M. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742.
2. Ahlswede, R.; Csiszár, I. Common Randomness in Information Theory and Cryptography—Part I: Secret Sharing. *IEEE Trans. Inf. Theory* **1993**, *39*, 1121–1132.
3. Bennett, C.H.; Brassard, G.; Robert, J.M. Privacy amplification by public discussion. *SIAM J. Comput.* **1988**, *17*, 210–229.
4. Shannon, C.E. A mathematical theory of communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423.
5. Gács, P.; Körner, J. Common information is far less than mutual information. *Probl. Control Inf. Theory* **1972**, *2*, 149–162.
6. Csiszár, I.; Narayan, P. Secrecy Capacities for Multiple Terminals. *IEEE Trans. Inf. Theory* **2004**, *50*, 3047–3061.
7. Csiszár, I.; Narayan, P. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory* **2000**, *46*, 344–366.
8. Watanabe, S.; Oohama, Y. Secret key agreement from correlated Gaussian sources by rate limited public communication. *IEICE Trans. Fundam. Electron. Comput. Sci.* **2010**, *93*, 1976–1983.
9. Watanabe, S.; Oohama, Y. Secret key agreement from vector Gaussian sources by rate limited public communication. *IEEE Trans. Inf. Forensic Secur.* **2011**, *6*, 541–550.
10. Liu, J.; Cuff, P.; Verdú, S. Key Capacity for Product Sources with Application to Stationary Gaussian Processes. *IEEE Trans. Inf. Theory* **2016**, *62*, 984–1005.
11. Tyagi, H. Common Information and Secret Key Capacity. *IEEE Trans. Inf. Theory* **2013**, *59*, 5627–5640.
12. Kaspi, A. Two-way source coding with a fidelity criterion. *IEEE Trans. Inf. Theory* **1985**, *31*, 735–740.
13. Liu, J.; Cuff, P.W.; Verdú, S. Common Randomness and Key Generation with Limited Interaction. *arXiv* **2004**, arXiv:1601.00899.
14. Ma, N.; Ishwar, P.; Gupta, P. Interactive Source Coding for Function Computation in Collocated Networks. *IEEE Trans. Inf. Theory* **2012**, *58*, 4289–4305.
15. Gohari, A.; Anantharam, V. Information-Theoretic Key Agreement of Multiple Terminals—Part I. *IEEE Trans. Inf. Theory* **2010**, *56*, 3973–3996.
16. Mukherjee, M.; Kashyap, N.; Sankarasubramaniam, Y. Achieving SK capacity in the source model: When must all terminals talk? In Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT), Honolulu, HI, USA, 29 June–4 July 2014; pp. 1156–1160.
17. Zhang, H.; Liang, Y.; Lai, L. Secret Key Capacity: Talk or Keep Silent? In Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT), Hong Kong, China, 14–19 June 2015; pp. 291–295.

18. Chan, C.; Al-Bashabsheh, A.; Zhou, Q.; Ding, N.; Liu, T.; Sprintson, A. Successive Omniscience. *IEEE Trans. Inf. Theory* **2016**, *62*, 3270–3289.
19. Courtade, T.A.; Halford, T.R. Coded Cooperative Data Exchange for a Secret Key. *IEEE Trans. Inf. Theory* **2016**, *62*, 3785–3795.
20. Mukherjee, M.; Chan, C.; Kashyap, N.; Zhou, Q. Bounds on the communication rate needed to achieve SK capacity in the hypergraphical source model. In Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 2504–2508.
21. Mukherjee, M.; Kashyap, N.; Sankarasubramaniam, Y. On the Public Communication Needed to Achieve SK Capacity in the Multiterminal Source Model. *IEEE Trans. Inf. Theory* **2016**, *62*, 3811–3830.
22. Chan, C.; Mukherjee, M.; Kashyap, N.; Zhou, Q. When is omniscience a rate-optimal strategy for achieving secret key capacity? In Proceedings of the IEEE Information Theory Workshop, London, UK, 11–14 September 2016; doi:10.1109/ITW.2016.7606855.
23. Nitinawarat, S.; Narayan, P. Perfect Omniscience, Perfect Secrecy, and Steiner Tree Packing. *IEEE Trans. Inf. Theory* **2010**, *56*, 6490–6500.
24. Chan, C.; Zheng, L. Mutual Dependence for Secret Key Agreement. In Proceedings of 44th Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 17–19 March 2010.
25. Chan, C.; Mukherjee, M.; Kashyap, N.; Zhou, Q. On the Optimality of Secret Key Agreement via Omniscience. *arXiv* **2017**, arXiv:1702.07429.
26. Chan, C.; Mukherjee, M.; Kashyap, N.; Zhou, Q. Secret key agreement under discussion rate constraints. In Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT), Aachen, Germany, 25–30 June 2017; pp. 1519–1523.
27. Nitinawarat, S.; Ye, C.; Barg, A.; Narayan, P.; Reznik, A. Secret Key Generation for a Pairwise Independent Network Model. *IEEE Trans. Inf. Theory* **2010**, *56*, 6482–6489.
28. Chan, C.; Al-Bashabsheh, A.; Zhou, Q. Incremental and decremental secret key agreement. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 2514–2518.
29. Chan, C.; Al-Bashabsheh, A.; Zhou, Q. Change of Multivariate Mutual Information: From Local to Global. *IEEE Trans. Inf. Theory* **2017**, doi:10.1109/TIT.2017.2749372.
30. Nitinawarat, S.; Narayan, P. Secret Key Generation for Correlated Gaussian Sources. *IEEE Trans. Inf. Theory* **2012**, *58*, 3373–3391.
31. Vatedka, S.; Kashyap, N. A lattice coding scheme for secret key generation from Gaussian Markov tree sources. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 515–519.
32. Chan, C.; Al-Babsheh, A.; Ebrahimi, J.; Kaced, T.; Liu, T. Multivariate Mutual Information Inspired by Secret-Key Agreement. *Proc. IEEE* **2015**, *103*, 1883–1913.
33. Chan, C. On Tightness of Mutual Dependence Upperbound for Secret-key Capacity of Multiple Terminals. *arXiv* **2008**, arXiv:0805.3200.
34. Chan, C. The Hidden Flow of Information. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), St. Petersburg, Russia, 31 July–5 August 2011.
35. Chan, C. Matroidal undirected network. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Honolulu, HI, USA, 28–31 October 2012; pp. 1498–1502.
36. Chan, C.; Al-Bashabsheh, A.; Zhou, Q.; Kaced, T.; Liu, T. Info-Clustering: A Mathematical Theory for Data Clustering. *IEEE Trans. Mol. Biol. Multi-Scale Commun.* **2016**, *2*, 64–91.
37. Chan, C.; Al-Bashabsheh, A.; Zhou, Q.; Liu, T. Duality between Feature Selection and Data Clustering. In Proceedings of the 54th Annual Allerton Conference on Communication, Control, and Computing, Allerton Retreat Center, Monticello, IL, USA, 27–30 September 2016.
38. Csiszár, I. Axiomatic characterizations of information measures. *Entropy* **2008**, *10*, 261–273.
39. Tishby, N.; Pereira, F.C.; Bialek, W. The information bottleneck method. *arXiv* **2000**, arXiv:physics/0004057.
40. Friedman, N.; Mosenzon, O.; Slonim, N.; Tishby, N. Multivariate information bottleneck. *Proceedings of the Seventeenth conference on Uncertainty in artificial intelligence*; Morgan Kaufmann: San Francisco, CA, USA, 2001; pp. 152–161.
41. Watanabe, S. Information Theoretical Analysis of Multivariate Correlation. *IBM J. Res. Dev.* **1960**, *4*, 66–82.

42. Csiszár, I.; Narayan, P. Secrecy Capacities for Multiterminal Channel Models. *IEEE Trans. Inf. Theory* **2008**, *54*, 2437–2452.
43. Erkip, E.; Cover, T.M. The efficiency of investment information. *IEEE Trans. Inf. Theory* **1998**, *44*, 1026–1040.
44. Tishby, N.; Zaslavsky, N. Deep learning and the information bottleneck principle. In Proceedings of the IEEE Information Theory Workshop, Jerusalem, Israel, 26 April–1 May 2015; doi:10.1109/ITW.2015.7133169.
45. Shwartz-Ziv, R.; Tishby, N. Opening the Black Box of Deep Neural Networks via Information. *arXiv* **2017**, arXiv:1703.00810.
46. Fujishige, S. Optimization over the polyhedron determined by a submodular function on a co-intersecting family. *Math. Program.* **1988**, *42*, 565–577.
47. Chan, C. Generating Secret in a Network. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2010.
48. Anantharam, V.; Gohari, A.; Kamath, S.; Nair, C. On maximal correlation, hypercontractivity, and the data processing inequality studied by Erkip and Cover. *arXiv* **2013**, arXiv:1304.6133.
49. Anantharam, V.; Gohari, A.; Kamath, S.; Nair, C. On hypercontractivity and a data processing inequality. In Proceedings of the IEEE International Symposium on Information Theory Proceedings (ISIT), Honolulu, HI, USA, 29 June–4 July 2014; pp. 3022–3026.
50. Huang, S.L.; Zheng, L. Linear information coupling problems. In Proceedings of the IEEE International Symposium on Information Theory (ISIT), Cambridge, MA, USA, 1–6 July 2012; pp. 1029–1033.