Minimal Public Communication for Maximum Rate Secret Key Generation

Himanshu Tyagi
Department of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland
College Park, MD-20742, USA
Email: tyagi@umd.edu

***Abstract*—Secret key generation is considered for a pair of terminals that observe correlated sources and communicate interactively over a public channel. It is argued that optimum rate secret key generation is linked inherently to the Wyner's notion of common information between two dependent random variables. The minimum rate of interactive public communication required to generate an optimum rate secret key is characterized in terms of a variant of this notion of common information.**

I. Introduction

Consider secret key (SK) generation by a pair of terminals that observe independent and identically distributed (i.i.d.) repetitions of two dependent random variables (rvs) of known distribution. It is assumed that the rvs are discrete and finite-valued. The terminals communicate over a public channel of unlimited capacity, interactively in multiple rounds, to agree upon the value of the key. This value is required to be almost independent of the observations of an eavesdropper with access to the public channel. The maximum rate of such an SK was characterized in [7], [1].

In this paper, we characterize the minimum overall rate of public communication required to establish a maximum rate SK. This question was raised in [4, Section VI]. While our main result does not constitute a single-letter characterization, it nonetheless reveals a central link between secrecy generation and Wyner's notion of common information (CI) between two dependent rvs [9]. CI was defined as the minimum rate of a function of i.i.d. repetitions of the rvs that facilitated a certain distributed source coding task. In [9], another interpretation was given in terms of the minimum rate of shared bits for generation of correlated sources. In [5], CI was related to the minimum number of shared bits required for distributed channel simulation. We introduce a variant of this notion of CI called the *interactive* CI where the minimum of the rate is taken over those functions in Wyner's definition that additionally can be recovered as "common randomness" [2]. Our main contribution is to establish a one-to-one correspondence between such functions and optimum rate secret keys. This correspondence is then used to characterize the aforementioned minimum communication rate for the generation of an optimum rate secret key. In fact, it is shown that this minimum rate is simply interactive CI minus the secret key capacity.

Basic notions of common randomness and SKs are explained in the next section. The definition of interactive CI and the heuristics for our approach are given in Section III. Our main result is proved in Section IV.

II. Interactive Communication, Common Randomness and Secret Keys

In this section, we review some pertinent definitions. Consider discrete rvs X and Y taking values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively. A discrete memoryless multiple source (DMMS) with two components generates n i.i.d. repetitions of X and Y, denoted respectively by X^n and Y^n. An *r-rounds interactive communication* $\mathbf{f} = (f_1, g_1, f_2, g_2, ..., f_r, g_r)$ is a sequence of finite valued mappings with

$$\begin{aligned} f_i &: \mathcal{X}^n \times \mathcal{F}^{i-1} \times \mathcal{G}^{i-1} \rightarrow \mathcal{F}_i, \\ g_i &: \mathcal{Y}^n \times \mathcal{F}^{i} \times \mathcal{G}^{i-1} \rightarrow \mathcal{G}_i, \quad 1 \leq i \leq r, \end{aligned}$$

where $\{\mathcal{F}_i, \mathcal{G}_i\}_{i=1}^r$ are finite sets and $\mathcal{F}_0 = \mathcal{G}_0 = \emptyset$. Let $\mathbf{F} = \mathbf{f}\left(X^n, Y^n\right)$ be the corresponding random variable. The rate of this communication is given by

$$\frac{1}{n} \log \|\mathbf{f}\|,$$

where $\|\mathbf{f}\|$ denotes the cardinality of the range space of $\mathbf{f}$. The communication is taken to be a deterministic function of the observations, i.e., randomization at the terminals is not allowed.

For interactive communication $\mathbf{F}$, a function L of (X^n, Y^n) is *ϵ_n-recoverable common randomness* (ϵ_n-CR), recoverable from $\mathbf{F}$, if there exist mappings $L_1 = L_1^{(n)}(X^n, \mathbf{F})$ and $L_2 = L_2^{(n)}(Y^n, \mathbf{F})$ such that

$$\Pr\left\{L = L_1 = L_2\right\} \geq 1 - \epsilon_n.$$

L is recoverable from $\mathbf{F}$ if it is ϵ_n-recoverable with $\lim_{n\rightarrow\infty} \epsilon_n = 0$.

A function K of (X^n, Y^n) forms an *ϵ_n-secret key* (ϵ_n-SK) if K is ϵ_n-CR recoverable from interactive public communication $\mathbf{F}$ and

$$\frac{1}{n} I(K \wedge \mathbf{F}) < \epsilon_n.$$

978-1-4577-0595-3/11/$26.00 ©2011 IEEE

The SK capacity C is the largest rate $\liminf_n (1/n)H\left(K^{(n)}\right)$ of ϵ_n-SKs as above, such that $\lim_{n\to\infty} \epsilon_n = 0$. The following result is well known.

Theorem 1. [7], [1] *The SK capacity is given by*

$$C = I(X \wedge Y).$$

III. Relation between Secret Key and Wyner's Common Information

We interpret Wyner's CI corresponding to a pair of rvs (X, Y) as the minimum rate of a function of i.i.d. repetitions of the rvs (X^n, Y^n) that renders them conditionally independent. Formally, given n i.i.d. repetitions of finite valued rvs X and Y, taking values in the sets $\mathcal{X}$ and $\mathcal{Y}$, respectively, consider a sequence of finite valued mappings $L = \left\{L^{(n)}\left(X^n, Y^n\right)\right\}$ that satisfy the following property:

$$\lim_{n\to\infty} \frac{1}{n} I\left(X^n \wedge Y^n \mid L^{(n)}\right) = 0. \tag{1}$$

A trivial such mapping L is the identity map $Id\left(X^n, Y^n\right) = (X^n, Y^n)$. The CI corresponding to a pair of rvs (X, Y) is defined as

$$CI(X,Y) := \inf_L \liminf_n \frac{1}{n} H\left(L^{(n)}\right), \tag{2}$$

where the infimum is taken over the set of all sequences of functions L satisfying (1). The definition in (2), though not stated explicitly in [9], follows from analysis therein. The following theorem characterizes $CI(X, Y)$.

Theorem 2. [9] *The CI of two rvs is given by*

$$CI(X,Y) = \min_W I(X, Y \wedge W), \tag{3}$$

where the rv W takes values in a finite set $\mathcal{W}$ with $|\mathcal{W}| \leq |\mathcal{X}||\mathcal{Y}|$ and satisfies the Markov condition $X -\!\!\circ\!\!- W -\!\!\circ\!\!- Y$.

The direct part follows from [9, equation 5.12]. The proof of converse is straightforward.

The rvs L satisfying (1) have a special role in SK generation. While generating an SK K, if the terminals have recovered L as CR, then they cannot augment K further with another SK that is independent of L; therefore, such a K is maximal. However, to recover L as a CR at the terminals observing X^n and Y^n, interactive public communication is needed. The overall CR established now should also include $\mathbf{F}$. Inspired by this we have the following definition.

Definition 1. Let $\mathbf{F}$ be an r-rounds interactive communication and J be an ϵ_n-CR recoverable from $\mathbf{F}$, for some $\epsilon_n \to 0$. Further assume that the function L of (X^n, Y^n) defined by $L = (J, \mathbf{F})$ satisfies (1). The *r-rounds interactive common information* $CI_i^r(X,Y)$ is defined as the infimum in (2) taken over all such L.

Remark. By definition, the nonnegative sequence $CI_i^r(X,Y)$ is nonincreasing with increasing r and is bounded below by $CI(X, Y)$. Define

$$CI_i(X,Y) = \lim_{r\to\infty} CI_i^r(X,Y).$$

Then $CI_i(X,Y) \geq CI(X,Y) \geq 0$. Further, since $L = X^n$ satisfies (1) and can be recovered from Y^n and a communication $F = F(X^n)$, $CI_i(X,Y) \leq H(X)$. Similarly, $CI_i(X,Y) \leq H(Y)$. To summarize, we have

$$0 \leq CI(X,Y) \leq CI_i(X,Y) \leq \min\{H(X), H(Y)\},$$

where each inequality above can be shown to be strict.

Out main result asserts the following. *An interactive CR that satisfies (1) can be used to generate an optimum rate SK and conversely, an optimum rate SK yields an interactive CR satisfying (1). In fact, such a CR of rate R can be recovered from an interactive communication of rate $R - C$, where C is the SK capacity. Therefore, to find the minimum rate of interactive communication needed to generate an optimum rate SK it is sufficient to characterize $CI_i(X,Y)$.*

IV. Main Result

Let R_{CI}^r be the infimum of the rate of r-rounds interactive communication $\mathbf{F}$ such that, for some $\epsilon_n \geq 0$ with $\epsilon_n \to 0$, some J is ϵ_n-CR recoverable from $\mathbf{F}$ and $L = (J, \mathbf{F})$ satisfies (1). Similarly, let R_{SK}^r be the infimum of the rate of r-rounds interactive communication $\mathbf{F}$ such that, for some $\epsilon_n \geq 0$, $\epsilon_n \to 0$, a sequence K of SKs of rate $C = I(X \wedge Y)$ can be generated using $\mathbf{F}$. Note that by their definitions, both R_{CI}^r and R_{SK}^r are nonincreasing with increasing r. Since both the sequences are also bounded below by zero, they converge to nonnegative limits R_{CI} and R_{SK} respectively. The following theorem constitutes our main result.

Theorem 3.

$$R_{SK} = R_{CI} = CI_i(X,Y) - I(X \wedge Y). \tag{4}$$

Remark. Theorem 3 can be interpreted as follows. Any CR J that is recoverable from a communication $\mathbf{F}$, with $L = (J, \mathbf{F})$ satisfying (1), can be decomposed into two mutually independent parts: An SK K of optimum rate and the interactive communication $\mathbf{F}$. Rewriting equation (4) as $CI_i(X,Y) = I(X \wedge Y) + R_{CI}$, for such a CR L of rate $CI_i(X,Y)$, this communication $\mathbf{F}$ is of rate R_{CI}. Furthermore, R_{CI} is same as R_{SK}. In fact, the proof of Theorem 3 entails showing a structural equivalence between a CR L as above and an optimum rate SK.

Theorem 3 follows from the following Lemma.

Lemma 4. *For each $r \geq 1$, the following inequalities hold*

$$R_{SK}^r \geq R_{CI}^r \geq R_{SK}^{r+1} \tag{5}$$

$$R_{CI}^r \geq CI_i^r(X,Y) - I(X \wedge Y) \geq R_{CI}^{r+1}. \tag{6}$$

Theorem 3 is proved by taking the limit $r \to \infty$ in (5) and (6).

A computable characterization of the operational term $CI_i(X,Y)$ is not known. The next result, however, gives a characterization of $CI_i^r(X,Y)$.

Lemma 5. *Given rvs X, Y and $r \geq 1$, we have*

$$CI_i^r(X,Y) = \min_{U_1,V_1,...,U_r,V_r} I(X,Y \wedge U_1,V_1,...,U_r,V_r), \tag{7}$$

where the minimum is taken over rvs $U_1, V_1..., U_r, V_r$ taking values in sets finite sets $\mathcal{U}_1, \mathcal{V}_1, ..., \mathcal{U}_r, \mathcal{V}_r$, respectively, that satisfy the following conditions

$$\begin{aligned}
&(i)\, U_i -\!\circ\!- X, U^{i-1}, V^{i-1} -\!\circ\!- Y \\
&\quad V_i -\!\circ\!- Y, U^i, V^{i-1} -\!\circ\!- X, \quad 1 \leq i \leq r, \\
&(ii)\, X -\!\circ\!- U^r, V^r -\!\circ\!- Y \\
&(iii)\, |\mathcal{U}_i| \leq |\mathcal{X}| \prod_{j=1}^{i-1} |\mathcal{U}_j||\mathcal{V}_j| + 1 \\
&\quad |\mathcal{V}_i| \leq |\mathcal{Y}||\mathcal{U}_i| \prod_{j=1}^{i-1} |\mathcal{U}_j||\mathcal{V}_j| + 1, \quad 1 \leq i \leq r,
\end{aligned}$$

with $\mathcal{U}_0 = \mathcal{V}_0 = \emptyset$ and $U_0 = V_0 =$ constant. Here U^i denotes the rvs $(U_1, ..., U_i)$.

Remarks. (i) Note that (7) has the same form as (3) with W replaced by $(U_1, V_1, ..., U_r, V_r)$ satisfying the conditions above.

(ii) In this paper, we have considered interactive communication with an even number of interactions. However, a similar analysis can be extended to the case of an odd number of interactions. In particular, when only one terminal is allowed to communicate, the minimum rate of public communication R_{SK}^{one} required to generate an SK of rate C is given by

$$\begin{aligned}
R_{SK}^{one} &= \min_U I(X, Y \wedge U) - I(X \wedge Y) \\
&= \min_U I(X \wedge U) - I(X \wedge Y),
\end{aligned}$$

where the $\mathcal{U}$ valued rv U satisfies $U -\!\circ\!- X -\!\circ\!- Y$, $X -\!\circ\!- U -\!\circ\!- Y$ and $|\mathcal{U}| \leq |\mathcal{X}| + 1$.

A. Proof of Lemma 4

For an r-rounds interactive communication $\mathbf{F}$ and an arbitrary function J of (X^n, Y^n) the following equality holds

$$\begin{aligned}
I(X \wedge Y) = &\frac{1}{n}\big[I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) + H(J, \mathbf{F}) \\
&- H(J \mid \mathbf{F}, X^n) - H(J \mid \mathbf{F}, Y^n) \\
&- H(\mathbf{F} \mid X^n) - H(\mathbf{F} \mid Y^n)\big].
\end{aligned} \tag{8}$$

The proof of (8) follows readily upon rewriting the terms on the right side and is omitted here. This equality is the central tool for our proofs. We now prove (5) and (6).

(i) $R_{CI}^r \geq CI_i^r(X,Y) - I(X \wedge Y)$*:*

Let J be an ϵ_n-CR recoverable from $\mathbf{F}$. Using the Fano's inequality we have

$$\frac{1}{n}\big[H(J \mid \mathbf{F}, X^n) + H(J \mid \mathbf{F}, Y^n)\big] \leq 2\epsilon_n \log |\mathcal{X}||\mathcal{Y}| + \frac{2}{n}. \tag{9}$$

Further assume that L defined by $L = (J, \mathbf{F})$ satisfies (1). This assumption and (9) together with (8) yield

$$\begin{aligned}
&\left|\frac{1}{n}\big[H(J, \mathbf{F}) - H(\mathbf{F} \mid X^n) - H(\mathbf{F} \mid Y^n)\big] - I(X \wedge Y)\right| \\
&\leq 2\epsilon_n \log |\mathcal{X}||\mathcal{Y}| + \epsilon_n + \frac{1}{n}.
\end{aligned}$$

Since $H(\mathbf{F}) \geq H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)$, as can be seen upon rewriting the right side in terms of the components of $\mathbf{F}$, we have

$$\frac{1}{n}H(J, \mathbf{F}) - I(X \wedge Y) \leq H(\mathbf{F}) + 2\epsilon_n \log |\mathcal{X}||\mathcal{Y}| + \epsilon_n + \frac{2}{n},$$

which gives $CI_i^r(X,Y) - I(X \wedge Y) \leq R_{CI}^r$.

(ii) $R_{SK}^r \geq R_{CI}^r$*:*

Let K be an ϵ_n-SK recoverable from r-rounds interactive communication $\mathbf{F}$, $\epsilon_n \to 0$, satisfying

$$\frac{1}{n}H(K) \geq I(X \wedge Y) - \delta, \tag{10}$$

for an arbitrary fixed $\delta > 0$ and n sufficiently large. Substituting $J = K$ in (8), Fano's inequality, (10) and the fact that $(1/n)I(K \wedge \mathbf{F}) \leq \epsilon_n$ imply

$$\begin{aligned}
\frac{1}{n}I(X^n \wedge Y^n \mid K, \mathbf{F}) &\leq \big[I(X \wedge Y) - \frac{1}{n}H(K)\big] \\
&\quad + \frac{1}{n}\big[H(\mathbf{F}) - H(\mathbf{F} \mid K)\big] \\
&\quad + 2\epsilon_n \log |\mathcal{X}||\mathcal{Y}| + \frac{2}{n} \\
&\leq 2\delta,
\end{aligned}$$

for all n sufficiently large. Hence $L = (K, \mathbf{F})$ satisfies (1) implying that the rate of $\mathbf{F}$ is greater than R_{CI}^r. Since $\mathbf{F}$ was an arbitrary r-rounds interactive communication that generates an optimum rate SK , the claimed inequality follows.

(iii) $CI_i^r(X,Y) - I(X \wedge Y) \geq R_{CI}^{r+1}$*:*

Consider a sequence of ϵ_n-CR J that is recoverable from r-rounds interactive communication $\mathbf{F}$, such that $L = (J, \mathbf{F})$ satisfies (1). Assume that $(J, \mathbf{F})$ achieves $CI_i^r(X,Y)$. Given $\delta > 0$, Fano's inequality along with (8) gives

$$\frac{1}{n}\big[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\big] \leq CI_i^r(X,Y) - I(X \wedge Y) + \delta, \tag{11}$$

for n sufficiently large. Denote by J_1 and J_2 the estimates of J formed at the terminals observing X^n and Y^n, respectively. Note that since $L = (J, \mathbf{F})$ satisfies (1) and J is an ϵ_n-CR, for all $k \geq 1$

$$\frac{1}{kn}I\left(X^{nk} \wedge Y^{nk} \mid J_1^k, \mathbf{F}^k\right) \leq \delta,$$

for sufficiently large n. We show that by choosing $k = k(n)$ sufficiently large, we can find an $(r+1)$-rounds interactive communication $\mathbf{F}' = \mathbf{F}'\left(X^{nk}, Y^{nk}\right)$ of rate less than

$$\frac{1}{n}\big[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\big] + \delta,$$

where the rate is defined with respect to block-length nk, such that $(J_1^k, \mathbf{F}^k)$ form a δ-CR recoverable from $\mathbf{F}'$. Specifically we construct a communication $\mathbf{F}'$ that is a function of $(J_1^k, \mathbf{F}^k)$ and therefore

$$\frac{1}{kn} I\left(X^{nk} \wedge Y^{nk} \mid J_1^k, \mathbf{F}^k\right) = \frac{1}{kn} I\left(X^{nk} \wedge Y^{nk} \mid J_1^k, \mathbf{F}^k, \mathbf{F}'\right) < \delta.$$

It follows that

$$R_{CI}^{r+1} \leq \frac{1}{n}\big[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\big] + \delta,$$

which with (11) gives the required inequality.

It now remains to construct the $(r+1)$-rounds interactive communication $\mathbf{F}'$. To that end, observe that for k sufficiently large, [8] guarantees the existence of distributed source codes of rate less than

$$\frac{1}{n}\big[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\big] + \frac{\delta}{2},$$

which are function of $\mathbf{F}$ and allow both the terminals to reconstruct $\mathbf{F}$ with probability of error less than $(\delta/2)$. Note that we need $2r$ such codes, each corresponding to one interaction and together constituting the first r-rounds of $\mathbf{F}'$. This allows the construction of $J_{11}, ..., J_{1k}$ at the terminal observing X^n and $J_{21}, ..., J_{2k}$ at the terminal observing Y^n with probability of error less than $(\delta/2)$. Here $J_{1i} = J_1\left(X_{n(i-1)+1}^{ni}, Y_{n(i-1)+1}^{ni}\right)$ and $J_{2i} = J_2\left(X_{n(i-1)+1}^{ni}, Y_{n(i-1)+1}^{ni}\right)$ are k i.i.d. repetitions of rvs (J_1, J_2). Since J_1 and J_2 are estimates at each terminal of the ϵ_n-CR J, Fano's inequality implies

$$\frac{1}{n} H(J_1 \mid J_2) \leq \epsilon_n \log |\mathcal{X}||\mathcal{Y}| + \frac{1}{n}.$$

Using [8] once again, for n and k sufficiently large, there exists a function $f_{r+1} = f_{r+1}(J_1^k)$ of rate less than $(\delta/2)$ such that terminal with J_2^k can recover J_1^k with error probability less than $(\delta/2)$. Therefore, we have the required $(r+1)$-rounds communication scheme.

(iv) $R_{CI}^r \geq R_{SK}^{r+1}$:

Given a sequence of ϵ_n-CR J that is recoverable from r-rounds interactive communication $\mathbf{F}$ of rate $R_{\mathbf{F}}$, with $L = (J, \mathbf{F})$ satisfying (1). Using the analysis of the last part, for a fixed $\delta > 0$, for sufficiently large n and k, there exists an $(r+1)$-rounds interactive communication $\mathbf{F}' = \mathbf{F}'\left(X^{nk}, Y^{nk}\right)$ of rate $R_{\mathbf{F}'}$ satisfying

$$R_{\mathbf{F}'} \leq \frac{1}{n}\big[H(\mathbf{F} \mid X^n) + H(\mathbf{F} \mid Y^n)\big] + \delta, \tag{12}$$

such that $(J_1^k, \mathbf{F}^k)$ forms a δ-CR recoverable from $\mathbf{F}'$. Using the "balanced coloring lemma" [4, Lemma B.2] there exists a function $K = K(J_1^k, \mathbf{F}^k)$ which forms an SK of rate greater than

$$\begin{aligned}&\frac{1}{nk} H(J_1^k, \mathbf{F}^k) - R_{\mathbf{F}'} - \delta \\ &\geq \frac{1}{n}\big[H(J_1, \mathbf{F}) - H(\mathbf{F} \mid X^n) - H(\mathbf{F} \mid Y^n)\big] - 2\delta \\ &\geq I(X \wedge Y) - 3\delta,\end{aligned}$$

where the final inequality holds using the definition of J_1 and $\mathbf{F}'$ along with (8), for n sufficiently large. Therefore, $R_{\mathbf{F}'}$ is greater than R_{SK}^{r+1}. But from (12) we have

$$R_{\mathbf{F}'} \leq R_{\mathbf{F}} + \delta.$$

The proof can be completed by choosing $R_{\mathbf{F}} \leq R_{CI}^r + \delta$ and letting δ approach zero. □

B. Outline of Proof of Lemma 5

We first address the achievability part. Consider rvs $U_1, V_1, ..., U_r, V_r$ satisfying the conditions (i)-(iii) of Lemma 5. We show that for any $\delta > 0$, there exists δ-CR $J = J(X^n, Y^n)$, recoverable from r-rounds interactive communication $\mathbf{F}$ of rate $R_{\mathbf{F}}$ such that $L = (J, \mathbf{F})$ satisfies (1) and the cardinality $\|L\|$ of the range of L satisfies

$$\frac{1}{n} \log \|L\| \leq I\left(X, Y \wedge U^r, V^r\right) + 2\delta, \tag{13}$$

whenever n is sufficiently large. The communication $\mathbf{F}$ used to recover J will itself be a function of J and the entropy of J will satisfy

$$\frac{1}{n} H(J, \mathbf{F}) = \frac{1}{n} H(J) \geq I\left(X, Y \wedge U_1^r, V_1^r\right) + \delta, \tag{14}$$

for n sufficiently large. This condition says that J is almost uniformly distributed. Furthermore, the rate $R_{\mathbf{F}}$ will be chosen such that

$$R_{\mathbf{F}} \leq I\left(X, Y \wedge U^r, V^r\right) - I(X \wedge Y) + \delta. \tag{15}$$

Using conditions (14-15) with (8) we get

$$\begin{aligned}\frac{1}{n} I\left(X^n \wedge Y^n \mid J, \mathbf{F}\right) &\leq I(X \wedge Y) - \left[\frac{1}{n} H(J) - R_{\mathbf{F}}\right] + \Delta(\delta) \\ &\leq \Delta(\delta),\end{aligned}$$

where $\Delta(\delta) \to 0$ as $\delta \to 0$. Therefore, L satisfies (1). It remains to show that $(J, \mathbf{F})$ satisfying (14-15) can be constructed for n sufficiently large.

We use the interactive extension of the Wyner-Ziv coding described, for instance, in [6]. Here we shall describe briefly the scheme and point out the required properties. For each $1 \leq k \leq r$, let (R_{1k}, R_{2k}) satisfy

$$R_{1k} > I(X \wedge U_k \mid U^{k-1}, V^{k-1}) + \frac{\delta}{r}, \tag{16}$$

$$R_{2k} > I(Y \wedge V_k \mid U^k, V^{k-1}) + \frac{\delta}{r}. \tag{17}$$

For fixed $1 \leq a_i \leq 2^{nR_{1i}}$ and $1 \leq b_i \leq 2^{nR_{2i}}$ for $1 \leq i \leq k-1$ the sequences $\{\mathbf{u}_k(1), ..., \mathbf{u}_k(2^{nR_{1k}})\}$ are selected from the conditional typical set (see, for instance, [3]) $\mathcal{T}^n_{U_k|U_1^{k-1}, V_1^{k-1}}(\mathbf{u}_1(a_1), ..., \mathbf{v}_{k-1}(b_{k-1}))$. The communication f_k is a function of the index a_k and it bins the index into $I(X_k^U \mid U^{k-1}, V^{k-1}, Y) + (\delta/2r)$ bins. Similarly, for a fixed $1 \leq a_k \leq 2^{nR_{1k}}$, the sequences $\{\mathbf{v}_k(1), ..., \mathbf{v}_k(2^{nR_{2k}})\}$ are selected from $\mathcal{T}^n_{V_k|U_1^k, V_1^{k-1}}(\mathbf{u}_1(a_1), ..., \mathbf{v}_{k-1}(b_{k-1}), \mathbf{u}_k(a_k))$. The communication g_k is a function of the index b_k and it bins the index into $I(Y_k^V \mid U^k, V^{k-1}, X) + (\delta/2r)$ bins.

Knowing the previous indices $a_1, ..., b_{k-1}$, the terminal observing X^n finds the unique index a_k such that $(X^n, \mathbf{u}_1(a_1), ..., \mathbf{v}_{k-1}(b_{k-1})), \mathbf{u}_k(a_k)$ are jointly typical and sends the corresponding $f_k(a_k)$. If no such unique index can be found, an encoding error occurs and a_k is chosen as 1. The index b_k corresponding to Y^n and $a_1, ..., b_{k-1}, a_k$ is found similarly and $g_k(b_k)$ is sent. At the end of r-rounds both the terminals form an estimate of the CR J which corresponds to the index $a_1, b_1, ..., a_r, b_r$. It can be shown that for sufficiently large n, such codebook sequences can be selected for which J is a δ-CR recoverable from the communication defined above (see [9], [6]). The overall rate of communication is given by

$$\begin{aligned} R_{\mathbf{F}} = \sum_{k=1}^{r} \big[& I(X \wedge U_k \,| U^{k-1}, V^{k-1}, Y) \\ & + I(Y \wedge V_k \mid U^k, V^{k-1}, X) \big] + \delta. \end{aligned} \tag{18}$$

Note that (16-17) imply (13). Equation (15) follows from (18) and conditions (i)-(ii) of the Lemma, since

$$\begin{aligned} & I(X, Y \wedge U^r, V^r) - \sum_{k=1}^{r} \big[I(X \wedge U_k \mid U^{k-1}, V^{k-1}, Y) \\ & \qquad + I(Y \wedge V_k \mid U^k, V^{k-1}, X) \big] \\ & = \sum_{k=1}^{r} \big[I(Y \wedge U_k \mid U^{k-1}, V^{k-1}) + I(X \wedge V_k \mid U^k, V^{k-1}) \big] \\ & \quad + I(X \wedge Y) - I(X \wedge Y) \\ & = \sum_{k=2}^{r} \big[I(Y \wedge U_k \mid U^{k-1}, V^{k-1}) + I(X \wedge V_k \mid U^k, V^{k-1}) \big] \\ & \quad + I(X \wedge Y) + I(X \wedge V_1 \mid U_1) + I(Y \wedge U_1) - I(Y \wedge X) \\ & = \sum_{k=2}^{r} \big[I(Y \wedge U_k \mid U^{k-1}, V^{k-1}) + I(X \wedge V_k \mid U^k, V^{k-1}) \big] \\ & \quad + I(X \wedge Y) - I(Y \wedge X \mid U_1, V_1) = \ldots = \\ & = I(X \wedge Y). \end{aligned}$$

It remains to verify (14). For a fixed $(a_1, b_1, ..., a_r, b_r)$, it can be shown that the conditional probability of the event $\{J = (a_1, b_1, ..., a_r, b_r)\}$ given that no encoding error occurs is bounded above by

$$2^{-n\left[I(X, Y \wedge U^r, V^r) + \frac{\delta}{2}\right]},$$

which implies (14) for large n as the probability of encoding error goes to zero.

For the converse consider an ϵ_n-CR J, recoverable from an r-rounds interactive communication $\mathbf{F}$. Denote by J_2 the estimate of J at the terminal observing Y^n. Here $\epsilon_n \to 0$ as $n \to \infty$. For a fixed n, define T as a uniformly distributed rv over $\{1, ..., n\}$. Let rvs U_1^r, V_1^r be defined as

$$\begin{aligned} U_1 &= f_1, X^{T-1}, Y_{T+1}^n, T, \\ U_i &= f_i, \qquad 2 \le i \le r. \\ V_i &= g_i, \qquad 1 \le i < r, \\ V_r &= g_r, J_2, \end{aligned}$$

where Y_j^i denotes the rvs $(Y_j, ..., Y_i)$. This definition of U_1^r, V_1^r satisfies (i) using [6, equations (3.10)-(3.13)]. Next observe that for some $\delta_n \to 0$

$$\begin{aligned} \delta_n \ge \frac{1}{n} I(X^n \wedge Y^n \mid J, \mathbf{F}) & \ge \frac{1}{n} I(X^n \wedge Y^n \mid J_2, \mathbf{F}) - \delta_n \\ & = I\left(X_T \wedge Y^n \mid J_2, \mathbf{F}, X^{T-1}, T\right) - \delta_n \\ & = I\left(X^n \wedge Y_T \mid J_2, \mathbf{F}, Y_{T+1}^n, T\right) - \delta_n, \end{aligned}$$

implying

$$I(X_T \wedge Y_T \mid U^r, V^r) \le \delta_n, \tag{19}$$

$$I\left(X_T \wedge Y_T^n \mid J_2, \mathbf{F}, X^{T-1}, T\right) \le \delta_n, \tag{20}$$

$$I\left(X_{T+1}^n \wedge Y_T \mid J_2, \mathbf{F}, Y_{T+1}^n, X^T, T\right) \le \delta_n. \tag{21}$$

The entropy rate of $(J, \mathbf{F})$ is now bounded as

$$\begin{aligned} & \frac{1}{n} H(J, \mathbf{F}) \\ & \ge \frac{1}{n} H(J_2, \mathbf{F}) - \delta_n \ge \frac{1}{n} I(X^n, Y^n \wedge J_2, \mathbf{F}) - \delta_n \\ & = H(X_T, Y_T) - H\left(X_T \mid J_2, \mathbf{F}, X^{T-1}, T\right) \\ & \quad - H\left(Y_T \mid J_2, \mathbf{F}, Y_{T+1}^n, X^{T-1}, T, X_T, X_{T+1}^n\right) - \delta_n, \end{aligned}$$

which with (20) and (21) gives

$$\frac{1}{n} H(J, \mathbf{F}) \ge I(X_T, Y_T \wedge U^r, V^r) - 3\delta_n. \tag{22}$$

The proof is now completed by interchanging rvs U^r, V^r by those of cardinalities bounded as in condition (iii), while still maintaining (19), (21) and the Markov chains in (i). This can be done using the support lemma [3, Lemma 3.4]. Finally, since the set of probability measures over finite and discrete rvs is compact, take the limit as $n \to \infty$ in (19) to get (ii) and in (21) to establish the converse.

ACKNOWLEDGEMENTS

The author thanks Prof. Prakash Narayan for his help in this research.
This work was supported by the U.S. National Science Foundation under Grants CCF0635271 and CCF0830697.

REFERENCES

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part i: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, 1993.

[2] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part ii: CR capacity," *IEEE Trans. Inform. Theory*, vol. 44, pp. 225–240, 1998.

[3] I. Csiszár and J. Körner, *Information theory: coding theorems for discrete memoryless channels*. Academic Press, 1981.

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

[5] P. Cuff, "Communication requirements for generating correlated random variables," *Proc. Int. Symp. Inform. Theory*, pp. 1393–1397, July 2008.

[6] A. H. Kaspi, "Two-way source coding with a fidelity criterion," *IEEE Trans. Inform. Theory*, vol. 31, no. 6, pp. 735–740, November 1985.

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.

[8] D. Slepian and J. Wolf, "Noiseless coding of correlated information source," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, 1973.

[9] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inform. Theory*, vol. 21, no. 2, pp. 163–179, March 1975.