How Many Queries Will Resolve Common Randomness?

Himanshu Tyagi and Prakash Narayan, *Fellow, IEEE*

***Abstract*—A set of m terminals, observing correlated signals, communicate interactively to generate common randomness for a given subset of them. Knowing only the communication, how many direct queries of the value of the common randomness will resolve it? A general upper bound, valid for arbitrary signal alphabets, is developed for the number of such queries by using a query strategy that applies to all common randomness and associated communication. When the underlying signals are independent and identically distributed repetitions of m correlated random variables, the number of queries can be exponential in signal length. For this case, the mentioned upper bound is tight and leads to a single-letter formula for the largest query exponent, which coincides with the secret key capacity of a corresponding multiterminal source model. In fact, the upper bound constitutes a strong converse for the optimum query exponent, and implies also a new strong converse for secret key capacity. A key tool, estimating the size of a large probability set in terms of Rényi entropy, is interpreted separately, too, as a lossless block coding result for general sources. As a particularization, it yields the classic result for a discrete memoryless source.**

***Index Terms*—Common randomness, Gaussian secret key capacity, interactive communication, query, query exponent, secret key capacity, strong converse.**

I. Introduction

A set of terminals observing correlated signals agree on common randomness (CR), i.e., shared bits, by communicating interactively among themselves. What is the maximum number of queries of the form "Is CR $= l$?" with yes-no answers that an observer of (only) the communication must ask in order to resolve the value of the CR? As an illustration, suppose that two terminals observe, respectively, n independent and identically distributed (i.i.d.) repetitions of the finite-valued random variables (rvs) X_1 and X_2. The terminals agree on CR X_1^n with terminal 1 communicating to terminal 2 a Slepian–Wolf codeword of rate $H(X_1 \mid X_2)$ obtained by random binning. An observer of the bin index can ascertain the value of CR with large probability in approximately $\exp\left[nI(X_1 \wedge X_2)\right]$ queries (corresponding to bin size). Our results show that more queries cannot be incurred by any other form of CR and associated interactive communication.

In a general setting, terminals $1, \ldots, m$ observe, respectively, n i.i.d. repetitions of the rvs $X_1, \ldots, X_m$, and communicate interactively to create CR, say L, for the terminals in a given subset $\mathcal{A} \subseteq \{1, \ldots, m\}$. For appropriate CR L and communication $\mathbf{F}$, the number of queries of the form "Is $L = l$?" that an observer of $\mathbf{F}$ must ask to resolve L is exponential in n. We find a single-letter formula for the largest exponent E^*. Remarkably, this formula coincides with the secret key (SK) capacity for a multiterminal source model with underlying rvs $X_1, \ldots, X_m$ [9], [10]. The latter is the largest rate of nearly uniformly distributed CR for $\mathcal{A}$ that meets the security requirement of being nearly independent of the communication used to generate it. While it is to be expected that E^* is no smaller than SK capacity, the less-restricted E^* may seem *a priori* to be larger. But it is not so. The coincidence brings out, in effect, an equivalence between inflicting a maximum number of queries on an observer of $\mathbf{F}$ on the one hand, and imposing the explicit secrecy constraint above on the other hand. In fact, as in the achievability proof of SK capacity in [9], the exponent E^* is achieved by the terminals in $\mathcal{A}$ attaining "omniscience," i.e., by generating CR $L = (X_1^n, \ldots, X_m^n)$ for $\mathcal{A}$, using communication $\mathbf{F}$ of minimum rate.

Alternatively, E^* can be interpreted as the smallest rate of a list of CR values produced by an observer of $\mathbf{F}$ which contains L with large probability.

Our main contribution is a new technique for proving converse results involving CR with interactive communication. It relies on query strategies for L given $\mathbf{F}$ that do not depend explicitly on the form of L or $\mathbf{F}$, and do not require the rvs $(X_{1t}, \ldots, X_{mt})_{t=1}^n$ to be finite-valued or i.i.d. In fact, our converse results hold even when the underlying alphabets are arbitrary, but under mild technical assumptions. Jointly Gaussian rvs are treated as a special case. Furthermore, our converses are strong in that the characterization of E^* does not depend on the probability of recovery of the CR. This, in turn, leads to a new strong converse result for the SK capacity of the multiterminal source model [9], [10]. A byproduct of our technique is a simple lossless block coding result for general finite sources, in terms of Rényi entropies. A particularization recovers the classic lossless block coding result for i.i.d. sources [24] without recourse to the asymptotic equipartition property (AEP).

The number of queries above can be interpreted as a measure of the correlation among the random signals observed by the terminals: A stronger correlation necessitates more queries for resolving the CR that can be generated by them. Such a measure of correlation is in the spirit of the body of work on "guessing"

Manuscript received November 06, 2012; revised April 29, 2013; accepted May 01, 2013 . Date of publication May 16, 2013; date of current version August 14, 2013. This work was supported by the U.S. National Science Foundation under Grants CCF0830697 and CCF1117546. The paper was presented at the 2013 IEEE International Symposium on Information Theory.

The authors are with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, College Park, MD 20742 USA (e-mail: tyagi@umd.edu; prakash@umd.edu).

Communicated by E. Arıkan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2013.2262496

the value of an rv based on a correlated observation [21], [2], [3], [14].

The problem formulation and our main result characterizing the optimum query exponent are given in the next section. Simple and essential technical tools which also may be of independent interest are presented in Section III. Achievability is proved in Section IV. The less complex converse proof for the case $\mathcal{A} = \{1, \ldots, m\}$ is given in Section V. However, this proof does not extend to an arbitrary $\mathcal{A} \subseteq \{1, \ldots, m\}$, for which a different converse is provided in Section VI. Section VII contains the strong converse result for SK capacity. A converse for the optimum query exponent for rvs with arbitrary alphabets is proved in Section VIII, with jointly Gaussian rvs as a special case. The discussion in Section IX includes the mentioned lossless block coding result for general sources.

II. Main Result

Let $X_1, \ldots, X_m$, $m \geq 2$, be rvs with finite alphabets $\mathcal{X}_1, \ldots, \mathcal{X}_m$, respectively, and with a known joint probability mass function (pmf) $\mathrm{P}_{X_1, \ldots, X_m}$. For any nonempty set $\mathcal{A} \subseteq \mathcal{M} = \{1, \ldots, m\}$, we denote $X_{\mathcal{A}} = (X_i,\ i \in \mathcal{A})$. We denote n i.i.d. repetitions of $X_{\mathcal{M}} = (X_1, \ldots, X_m)$ with values in $\mathcal{X}_{\mathcal{M}} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_m$ by $X_{\mathcal{M}}^n = (X_1^n, \ldots, X_m^n)$ with values in $\mathcal{X}_{\mathcal{M}}^n = \mathcal{X}_1^n \times \cdots \times \mathcal{X}_m^n$. Given $\epsilon > 0$, for rvs U, V, we say that U is ϵ*-recoverable* from V if $\mathrm{P}\left(U \neq f(V)\right) \leq \epsilon$ for some function $f(V)$ of V. The cardinality of the range of the rv U is denoted by $\|U\|$, and the complement of a set A by A^c. All logarithms and exponentials are with respect to the base 2.

We consider a multiterminal source model for generating CR using interactive communication. Terminals $1, \ldots, m$ observe, respectively, the sequences $X_1^n, \ldots, X_m^n$, of length n. The terminals in a given set $\mathcal{A} \subseteq \mathcal{M}$ wish to generate CR using communication over a noiseless channel, possibly interactively in several rounds.

Definition 1: Assume without any loss of generality that the communication of the terminals in $\mathcal{M}$ occurs in consecutive time slots in r rounds, where r can depend on n but is finite for every n. Such communication is described in terms of the mappings

$$f_{11}, \ldots, f_{1m}, f_{21}, \ldots, f_{2m}, \ldots, f_{r1}, \ldots, f_{rm},$$

with f_{ji} corresponding to a message in time slot j by terminal i, $1 \leq j \leq r$, $1 \leq i \leq m$; in general, f_{ji} is allowed to yield any function of X_i^n and of previous communication

$$\phi_{ji} = \{f_{kl} : k < j,\ l \in \mathcal{M} \text{ or } k = j,\ l < i\}.$$

The corresponding rvs are termed collectively as *interactive communication*

$$\mathbf{F} = \{F_{11}, \ldots, F_{1m}, F_{21}, \ldots, F_{2m}, \ldots, F_{r1}, \ldots, F_{rm}\},$$

where $\mathbf{F} = \mathbf{F}^{(n)}(X_{\mathcal{M}}^n)$; the rv corresponding to ϕ_{ji} is denoted by Φ_{ji}. Local randomization at the terminals is not considered here for ease of exposition. In fact, allowing such randomization does not improve our result; see Section IX-B.

Definition 2: Given interactive communication $\mathbf{F}$ as above, an rv $L = L^{(n)}\left(X_{\mathcal{M}}^n\right)$ is ϵ*-common randomness* (ϵ-CR) for $\mathcal{A}$ from $\mathbf{F}$ if it is ϵ-recoverable from $(X_i^n, \mathbf{F})$, $i \in \mathcal{A}$, i.e., if there exist rvs $L_i = L_i^{(n)}\left(X_i^n, \mathbf{F}\right)$, $i \in \mathcal{A}$, satisfying

$$\mathrm{P}\left(L_i = L,\ i \in \mathcal{A}\right) \geq 1 - \epsilon. \tag{1}$$

The rv L_i will be called an estimate of L at terminal $i \in \mathcal{A}$.

A querier observing the communication $\mathbf{F}$ wants to resolve the value of this CR L by asking questions of the form "Is $L = l$?" with yes–no answers. While queries of this form have been termed "guessing" [21], [2], [3], [14], we use the terminology "query" since our approach covers a broader class of query strategies; see Section IX-B.

Definition 3: For rvs U, V with values in the sets $\mathcal{U}, \mathcal{V}$, a *query strategy* q for U given $V = v$ is a bijection $q(\cdot|v) : \mathcal{U} \rightarrow \{1, \ldots, |\mathcal{U}|\}$, where the querier, upon observing $V = v$, asks the question "Is $U = u$?" in the $q(u|v)$th query.

Thus, a query strategy q for resolving a CR L on the basis of an observed communication $\mathbf{F} = \mathbf{i}$ is an ordering of the possible values of L. The terminals seek to generate a CR L for $\mathcal{A}$ using communication $\mathbf{F}$ so as to make the task of the querier observing $\mathbf{F}$ as onerous as possible. For instance, if L were to be independent of $\mathbf{F}$, then the querier necessarily must search exhaustively over the set of possible values of L, which can be exponentially large (in n).

Definition 4: Given $0 < \epsilon < 1$, a *query exponent* $E > 0$ is ϵ-achievable if for every $0 < \epsilon' < 1$, there exists an ϵ-CR $L = L^{(n)}\left(X_{\mathcal{M}}^n\right)$ for $\mathcal{A} \subseteq \mathcal{M}$ from communication $\mathbf{F} = \mathbf{F}\left(X_{\mathcal{M}}^n\right)$ such that for every query strategy q for L given $\mathbf{F}$

$$\mathrm{P}\big(q(L \mid \mathbf{F}) \geq \exp(nE)\big) > 1 - \epsilon', \tag{2}$$

for all $n \geq N(\epsilon, \epsilon')$. The ϵ-optimum query exponent, denoted $E^*(\epsilon)$, is the supremum of all ϵ-achievable query exponents; $E^*(\epsilon)$ is nondecreasing in ϵ. The *optimum query exponent* E^* is the infimum of $E^*(\epsilon)$ for $0 < \epsilon < 1$, i.e.,

$$E^* = \lim_{\epsilon \rightarrow 0} E^*(\epsilon).$$

Remark: Clearly, $0 \leq E^* \leq \log |\mathcal{X}_{\mathcal{M}}|$.

Condition (2) forces any query strategy adopted by the querier to have an exponential complexity (in n) with large probability; E^* is the largest value of the exponent that can be inflicted on the querier.

Our main result is a single-letter characterization of the optimum query exponent E^*. Let

$$\mathcal{B} = \left\{B \subsetneq \mathcal{M} : B \neq \emptyset, \mathcal{A} \nsubseteq B\right\}. \tag{3}$$

Let $\Lambda(\mathcal{A})$ be the set of all collections $\lambda = \{\lambda_B : B \in \mathcal{B}\}$ of weights $0 \leq \lambda_B \leq 1$, satisfying

$$\sum_{B \in \mathcal{B} : B \ni i} \lambda_B = 1, \quad i \in \mathcal{M}. \tag{4}$$

Every $\lambda \in \Lambda(\mathcal{A})$ is called a *fractional partition* of $\mathcal{M}$ (see [10], [18]–[20]).

Theorem 1: The optimum query exponent E^* equals

$$E^* = E^*(\epsilon) = H\left(X_{\mathcal{M}}\right) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right), \qquad 0 < \epsilon < 1. \tag{5}$$

Remarkably, the value of E^* coincides with the SK capacity of a multiterminal source model [9], [10]. The latter is the largest rate of a CR $K = K\left(X_{\mathcal{M}}^n\right)$ for $\mathcal{A}$ from communication $\mathbf{F}$, with K satisfying the "secrecy constraint" of [9]:

$$\lim_n s_{in}(K; \mathbf{F}) = 0, \tag{6}$$

where the security index s_{in} is given by

$$s_{in}(K; \mathbf{F}) = \log \|K\| - H(K \mid \mathbf{F}) = D\left(\mathrm{P}_{K,\mathbf{F}} \,\|\, \mathrm{P}_{\text{unif}} \times \mathrm{P}_{\mathbf{F}}\right), \tag{7}$$

with P_{unif} being the uniform pmf on $\{1, \ldots, \|K\|\}$. In fact, the achievability proof of Theorem 1 is straightforward and employs, in effect, an SK in forming an appropriate CR L. We show that for such a CR L, any query strategy is tantamount to an exhaustive search over the set of values of the SK, a feature that is apparent for a "perfect" SK with $I(K \wedge \mathbf{F}) = 0$. The difficult step in the proof of Theorem 1 is the converse part which involves an appropriate query strategy, for arbitrary L and $\mathbf{F}$, that limits the incurred query exponents. Our *strong* converse yields a uniform upper bound for $E^*(\epsilon)$, $0 < \epsilon < 1$.

We shall see that while the expression for E^* in (5) lends itself to the achievability proof of Theorem 1 in Section IV, alternative forms are suited better for the converse proof. For the latter, denoting

$$\lambda_{\mathtt{sum}} = \sum_{B \in \mathcal{B}} \lambda_B, \tag{8}$$

the expression (5) can be written also as

$$E^* = \min_{\lambda \in \Lambda(\mathcal{A})} \left[\sum_{B \in \mathcal{B}} \lambda_B H\left(X_{B^c}\right) - \left(\lambda_{\mathtt{sum}} - 1\right) H\left(X_{\mathcal{M}}\right)\right], \tag{9}$$

which is used in the converse proof for an arbitrary $\mathcal{A} \subseteq \mathcal{M}$ in Section VI. The converse proof for the case $\mathcal{A} = \mathcal{M}$ is facilitated by the fact that the right-side of (9) can be expressed equivalently as [7] (see also [9, Example 4])

$$\min_{\pi} \frac{1}{|\pi| - 1} D\left(\mathrm{P}_{X_{\mathcal{M}}} \,\|\, \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\right), \tag{10}$$

where the minimum is over all (nontrivial) partitions $\pi = (\pi_1, \ldots, \pi_k)$ of $\mathcal{M}$ with $|\pi| = k$ parts, $2 \leq k \leq m$.

III. Technical Tools

The following simple observation relates the number of queries in a query strategy q to the cardinality of an associated set.

Proposition 2: Let q be a query strategy for U given $V = v$, $v \in \mathcal{V}$. Then

$$|\{u \in \mathcal{U} : q(u|v) \leq \gamma\}| \leq \gamma.$$

Proof: The claim is straightforward since $q(\cdot|v)$ is a bijection. □

For rvs U, V, finding a lower bound for $q(U|V)$ involves finding a suitable upper bound for the conditional probabilities $\mathrm{P}_{U|V}(\cdot \mid \cdot)$. This idea is formalized by the following lemma.

Lemma 3: Given $\gamma > 0$ and $0 < \delta < 1/2$, let the rvs U, V, satisfy

$$\mathrm{P}\left(\left\{(u, v) : \mathrm{P}_{U|V}(u|v) \leq \frac{\delta}{\gamma}\right\}\right) \geq 1 - \delta. \tag{11}$$

Then, for every query strategy q for U given V,

$$\mathrm{P}\left(q(U|V) \geq \gamma\right) \geq 1 - \epsilon', \tag{12}$$

for all $\epsilon' \geq 2\delta$.

Conversely, if (12) holds for every query strategy q for U given V, with $0 < \epsilon' \leq (1 - \sqrt{\delta})^2$, then

$$\mathrm{P}\left(\left\{(u, v) : \mathrm{P}_{U|V}(u|v) \leq \frac{1}{\gamma}\right\}\right) \geq \delta. \tag{13}$$

Proof: Suppose (11) holds but not (12). Then, there exists q with

$$\mathrm{P}\left(q(U|V) < \gamma\right) > \epsilon'. \tag{14}$$

From (11) and (14)

$$\begin{aligned}\mathrm{P}&\left(\left\{(u, v) : \mathrm{P}_{U|V}(u|v) \leq \frac{\delta}{\gamma},\ q(u|v) < \gamma\right\}\right) \\ &> 1 - \delta + \epsilon' - 1 = \epsilon' - \delta.\end{aligned} \tag{15}$$

On the other hand, the left-side of (15) equals

$$\begin{aligned}&\sum_v \mathrm{P}_V(v) \sum_{u : q(u|v) < \gamma,\ \mathrm{P}_{U|V}(u|v) \leq \frac{\delta}{\gamma}} \mathrm{P}_{U|V}(u|v) \\ &\leq \gamma . \frac{\delta}{\gamma}, \qquad \text{by Proposition 2} \\ &= \delta,\end{aligned}$$

which contradicts (15) since $\epsilon' \geq 2\delta$.

For the converse, suppose that (13) does not hold; then, we show that a query strategy q_0 exists which violates (12) when $0 < \epsilon' \leq (1 - \sqrt{\delta})^2$. The negation of (13) is

$$\mathrm{P}\left(\left\{(u, v) : \mathrm{P}_{U|V}(u|v) > \frac{1}{\gamma}\right\}\right) > 1 - \delta,$$

which, by a reverse Markov inequality[1][17, p. 157] (see also [12, p. 153]), gives a set $\mathcal{V}_0 \subseteq \mathcal{V}$ with

$$\mathrm{P}_V\left(\mathcal{V}_0\right) > 1 - \sqrt{\delta}, \tag{16}$$

and

$$\mathrm{P}_{U|V}\left(\left\{(u : \mathrm{P}_{U|V}(u|v) > \frac{1}{\gamma}\right\} \,\Big|\, v\right) > 1 - \sqrt{\delta}, \quad v \in \mathcal{V}_0. \tag{17}$$

[1] The reverse Markov inequality states that for rvs U, V with $\mathrm{P}((U, V) \in S) \geq 1 - \epsilon$ for some $S \subseteq \mathcal{U} \times \mathcal{V}$, there exists $\mathcal{V}_0 \subseteq \mathcal{V}$ such that $\mathrm{P}((U, V) \in S \mid V = v) \geq 1 - \sqrt{\epsilon}$, $v \in \mathcal{V}_0$, and $\mathrm{P}(V \in \mathcal{V}_0) \geq 1 - \sqrt{\epsilon}$.

Denoting by $\mathcal{U}_v$ the set $\{\cdot\}$ in (17), we have

$$1 \geq \mathrm{P}_{U|V}\left(\mathcal{U}_v \mid v\right) > \frac{|\mathcal{U}_v|}{\gamma},$$

so that

$$|\mathcal{U}_v| < \gamma, \quad v \in \mathcal{V}_0. \tag{18}$$

For each $v \in \mathcal{V}_0$, order the elements of $\mathcal{U}$ arbitrarily but with the first $|\mathcal{U}_v|$ elements being from $\mathcal{U}_v$. This ordering defines a query strategy $q_0(\cdot|v)$, $v \in \mathcal{V}_0$; for $v \notin \mathcal{V}_0$, let $q_0(\cdot|v)$ be defined arbitrarily. Then for $v \in \mathcal{V}_0$, $u \in \mathcal{U}_v$,

$$q_0(u|v) < \gamma$$

by (18), so that

$$\begin{aligned}\mathrm{P}\left(q_0(U|V) < \gamma\right) &\geq \sum_{v \in \mathcal{V}_0} \sum_{u \in \mathcal{U}_v} \mathrm{P}_{U,V}\left(u, v\right) \\ &> (1-\sqrt{\delta})^2, \end{aligned} \tag{19}$$

by (16) and (17). So, $q = q_0$ violates (12) when $\epsilon' \leq (1-\sqrt{\delta})^2$. □

The next result relates the cardinalities of large probability sets to Rényi entropy. The first part is used in the converse proofs of Theorem 1. The mentioned result is of independent interest. For instance, in Section IX, it is shown to yield an elementary alternative proof of the source coding theorem for an i.i.d. (finite-valued) source.

Definition 5 [23]: Let μ be a nonnegative measure on $\mathcal{U}$. For $0 \leq \alpha \neq 1$, the *Rényi entropy of order* α of μ is defined as

$$H_\alpha(\mu) = \frac{1}{1-\alpha} \log \sum_{u \in \mathcal{U}} \mu(u)^\alpha.$$

Lemma 4:

(i) For every $0 < \delta < \mu(\mathcal{U})$, there exists a set $\mathcal{U}_\delta \subseteq \mathcal{U}$ such that

$$\mu\left(\mathcal{U}_\delta\right) \geq \mu(\mathcal{U}) - \delta, \tag{20}$$

and

$$|\mathcal{U}_\delta| \leq \delta^{-\alpha/(1-\alpha)} \exp\left(H_\alpha(\mu)\right), \qquad 0 \leq \alpha < 1. \tag{21}$$

(ii) Conversely, for $\delta, \delta' > 0$, $\delta + \delta' < \mu(\mathcal{U})$, any set $\mathcal{U}_\delta \subseteq \mathcal{U}$ with $\mu\left(\mathcal{U}_\delta\right)$ as in (20) must satisfy

$$|\mathcal{U}_\delta| \geq \left(\delta'\right)^{1/(\alpha-1)} \left(\mu(\mathcal{U}) - \delta - \delta'\right) \exp\left(H_\alpha(\mu)\right), \quad \alpha > 1. \tag{22}$$

Proof:

(i) For $0 \leq \alpha < 1$, defining

$$\mathcal{U}_\delta = \left\{u \in \mathcal{U} : \mu(u) > \delta^{\frac{1}{1-\alpha}} \exp\left[-H_\alpha(\mu)\right]\right\},$$

we get

$$\mu(\mathcal{U}) = \mu(\mathcal{U}_\delta) + \sum_{u:\ \mu(u) \leq \delta^{\frac{1}{1-\alpha}} \exp[-H_\alpha(\mu)]} \mu(u).$$

Writing the summand in the right-side above as $\mu(u) = \mu(u)^\alpha \mu(u)^{1-\alpha}$, we obtain

$$\begin{aligned}\mu(\mathcal{U}) &\leq \mu(\mathcal{U}_\delta) + \delta \exp\left[-(1-\alpha)H_\alpha(\mu)\right] \sum_{u \in \mathcal{U}} \mu(u)^\alpha \\ &= \mu\left(\mathcal{U}_\delta\right) + \delta,\end{aligned}$$

which is (20). Furthermore,

$$\begin{aligned}\exp\left[(1-\alpha)H_\alpha(\mu)\right] &= \sum_{u \in \mathcal{U}} \mu(u)^\alpha \\ &\geq \sum_{u \in \mathcal{U}_\delta} \mu(u)^\alpha \\ &\geq |\mathcal{U}_\delta| \delta^{\frac{\alpha}{1-\alpha}} \exp\left[-\alpha H_\alpha(\mu)\right],\end{aligned}$$

which gives (21).

(ii) By following the steps in the proof of (i), for $\alpha > 1$, it can be shown that the set

$$\mathcal{U}_0 = \left\{u \in \mathcal{U} : \mu(u) < \left(\delta'\right)^{1/(1-\alpha)} \exp[-H_\alpha(\mu)]\right\} \tag{23}$$

has

$$\mu(\mathcal{U}_0) > \mu(\mathcal{U}) - \delta',$$

which, with (20), gives

$$\mu(\mathcal{U}_0 \cap \mathcal{U}_\delta) > \mu(\mathcal{U}) - \delta - \delta'.$$

Since by (23)

$$\mu(\mathcal{U}_0 \cap \mathcal{U}_\delta) < |\mathcal{U}_0 \cap \mathcal{U}_\delta| \left(\delta'\right)^{1/(1-\alpha)} \exp[-H_\alpha(\mu)],$$

(22) follows.

□

Finally, the following simple observation will be useful.

Proposition 5: For pmfs Q_1, Q_2, on $\mathcal{V}$

$$Q_1\left(\{v : Q_1(v) \geq \delta Q_2(v)\}\right) \geq 1 - \delta, \qquad 0 < \delta < 1.$$

Proof: The claim follows from

$$\sum_{v \in \mathcal{V}: Q_1(v) < \delta Q_2(v)} Q_1(v) < \sum_{v \in \mathcal{V}: Q_1(v) < \delta Q_2(v)} \delta\, Q_2(v) \leq \delta.$$

□

IV. Achievability Proof of Theorem 1

Denoting the right-side of (5) by C, we claim, for $0 < \epsilon < 1$, $0 < \delta < 1/2$, $\beta > 0$, the existence of an ϵ-CR $L = X_{\mathcal{M}}^n$ for $\mathcal{A}$ from $\mathbf{F}$ with

$$\mathrm{P}\left(\left\{(x_{\mathcal{M}}^n, \mathbf{i}) : \mathrm{P}_{L|\mathbf{F}}\left(x_{\mathcal{M}}^n \mid \mathbf{i}\right) \leq \delta \exp\left[-n(C-\beta)\right]\right\}\right) \geq 1 - \delta, \tag{24}$$

for all n sufficiently large. Then, the assertion of the theorem follows by applying the first part of Lemma 3 with $U = L$, $V = \mathbf{F}, \gamma = \exp[n(C - \beta)]$, to conclude from (12) that

$$E^*(\epsilon) \geq C,$$

since $\beta > 0$ was chosen arbitrarily.

Turning to the mentioned claim, it is shown in [9, Prop. 1], [10, Th. 3.1] that there exists communication $\mathbf{F}$ such that $L = X_{\mathcal{M}}^n$ is ϵ-CR for $\mathcal{A}$ from $\mathbf{F}$ with

$$\frac{1}{n} \log \|\mathbf{F}\| \leq \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{B \in \mathcal{B}} \lambda_B H\left(X_B \mid X_{B^c}\right) + \frac{\beta}{3}, \tag{25}$$

for all n sufficiently large. Using Proposition 5 with $Q_1 = P_{\mathbf{F}}$ and Q_2 being the uniform pmf over the range of $\mathbf{F}$, we get

$$\mathrm{P}_{\mathbf{F}}\left(\left\{\mathbf{i} : \mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right) \geq \frac{\delta}{2\|\mathbf{F}\|}\right\}\right) \geq 1 - \frac{\delta}{2}. \tag{26}$$

Also, for $x_{\mathcal{M}}^n$ in the set $\mathcal{T}_n$ of $\mathrm{P}_{X_{\mathcal{M}}}$-typical sequences with constant δ [11, Definition 2.8], we have

$$\mathrm{P}_{X_{\mathcal{M}}^n}\left(x_{\mathcal{M}}^n\right) \leq \exp\left[-n\left(H\left(X_{\mathcal{M}}\right) - \frac{\beta}{3}\right)\right] \tag{27}$$

and

$$\mathrm{P}_{X_{\mathcal{M}}^n}\left(\mathcal{T}_n\right) \geq 1 - \frac{\delta}{2},$$

for all n sufficiently large. Denoting by $\mathcal{I}_0$ the set on the left-side of (26), it follows that

$$\mathrm{P}\left(X_{\mathcal{M}}^n \in \mathcal{T}_n, \mathbf{F} \in \mathcal{I}_0\right) \geq 1 - \delta. \tag{28}$$

The claim results from (26)–(28) upon observing that for $(x_{\mathcal{M}}^n, \mathbf{i}) \in \mathcal{T}^n \times \mathcal{I}_0$

$$\begin{aligned}\mathrm{P}_{X_{\mathcal{M}}^n|\mathbf{F}}\left(x_{\mathcal{M}}^n \mid \mathbf{i}\right) &= \frac{\mathrm{P}_{X_{\mathcal{M}}^n}\left(\left(x_{\mathcal{M}}^n\right)\right)\mathbf{1}\left(\mathbf{F}\left(x_{\mathcal{M}}^n\right) = \mathbf{i}\right)}{\mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right)} \\ &\leq \frac{2\exp\left[-n\left(H\left(X_{\mathcal{M}}\right) - \frac{\beta}{3}\right)\right]\|\mathbf{F}\|}{\delta} \\ &\leq \delta \exp[-n(C - \beta)],\end{aligned}$$

for all n large enough, where the last inequality is by (25). □

Remark: The achievability proof brings out a connection between a large probability uniform upper bound κ for P_L, the size $\|\mathbf{F}\|$ of the communication $\mathbf{F}$, and the associated number of queries needed. Loosely speaking, the number of queries is approximately $\frac{1}{\|\mathbf{F}\|\kappa}$, which reduces to $\frac{\|L\|}{\|\mathbf{F}\|}$ if L is nearly uniformly distributed.

V. Converse Proof of Theorem 1 for $\mathcal{A} = \mathcal{M}$

Recalling the expression for E^* in (10), given a partition π of $\mathcal{M}$ with $|\pi| = k$, $2 \leq k \leq m$, we observe that for a consolidated source model with k sources and underlying rvs $Y_1, \ldots, Y_k$ where[2] $Y_i = X_{\pi_i}$, the ϵ-optimum query exponent $E_\pi^*(\epsilon)$ can be no smaller than $E^*(\epsilon)$ (since the terminals in each π_i coalesce, in effect).

Theorem 6: For every partition π of $\mathcal{M}$ with $|\pi| = k$

$$E_\pi^*(\epsilon) \leq \frac{1}{k-1} D\Big(\mathrm{P}_{Y_1,\ldots,Y_k} \| \prod_{i=1}^{k} \mathrm{P}_{Y_i}\Big), \quad 0 < \epsilon < 1,$$

and so

$$E^*(\epsilon) \leq \min_\pi E_\pi^*(\epsilon) \leq \min_\pi \frac{1}{|\pi| - 1} D\Big(\mathrm{P}_{X_{\mathcal{M}}} \| \prod_{i=1}^{|\pi|} \mathrm{P}_{X_{\pi_i}}\Big).$$

Theorem 6 establishes, in view of (10), the converse part of Theorem 1 when $\mathcal{A} = \mathcal{M}$.

The proof of Theorem 6 relies on the following general result, which holds for queries of CR generated in a multiterminal source model with underlying rvs $Y_1, \ldots, Y_k$ for $n = 1$.

Theorem 7: Let $L = L\left(Y_1, \ldots, Y_k\right)$ be ϵ-CR for $\{1, \ldots, k\}$ from interactive communication $\mathbf{F} = \mathbf{F}\left(Y_1, \ldots, Y_k\right)$, $0 < \epsilon < 1$. Given $\delta > 0$ such that $\delta + \sqrt{\delta + \epsilon} < 1$, let θ be such that

$$\mathrm{P}\left(\left\{(y_1, \ldots, y_k) : \frac{\mathrm{P}_{Y_1,\ldots,Y_k}\left(y_1, \ldots, y_k\right)}{\prod_{i=1}^k \mathrm{P}_{Y_i}\left(y_i\right)} \leq \theta\right\}\right) \geq 1 - \delta. \tag{29}$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \geq (1 - \delta - \sqrt{\delta + \epsilon})^2. \tag{30}$$

Proof of Theorem 6: We apply Theorem 7 to n i.i.d. repetitions of the rvs $Y_1, \ldots, Y_k$. Denoting by $\mathcal{T}_n'$ the set of $\mathrm{P}_{Y_1,\ldots,Y_k}$-typical sequences with constant δ, we have

$$\mathrm{P}_{Y_1^n,\ldots,Y_k^n}\left(\mathcal{T}_n'\right) \geq 1 - \delta,$$

and for $(y_1^n, \ldots, y_k^n) \in \mathcal{T}_n'$

$$\begin{aligned}&\frac{\mathrm{P}_{Y_1^n,\ldots,Y_k^n}\left(y_1^n, \ldots, y_k^n\right)}{\prod_{i=1}^k \mathrm{P}_{Y_i^n}\left(y_i^n\right)} \\ &\leq \exp\left[n\Big(\sum_{i=1}^k H\left(Y_i\right) - H\left(Y_1, \ldots, Y_k\right) + \delta\Big)\right] \\ &= \exp\left[n\Big(D\Big(\mathrm{P}_{Y_1,\ldots,Y_k} \| \prod_{i=1}^k \mathrm{P}_{Y_i}\Big) + \delta\Big)\right],\end{aligned}$$

for all n large enough. Thus, the hypothesis of Theorem 7 holds with

$$\theta = \theta_n = \exp\left[n\Big(D\Big(\mathrm{P}_{Y_1,\ldots,Y_k} \| \prod_{i=1}^k \mathrm{P}_{Y_i}\Big) + \delta\Big)\right].$$

If E is an ϵ-achievable query exponent (see Definition 4), then there exists an ϵ-CR $L = L\left(Y_1^n, \ldots, Y_k^n\right)$ from communication $\mathbf{F} = \mathbf{F}\left(Y_1^n, \ldots, Y_k^n\right)$ such that (2) holds for the query strategy

[2] For specificity, the elements in each π_i are arranged in increasing order.

q_0 of Theorem 7 for this choice of L and $\mathbf{F}$. In particular for $\epsilon' < (1-\delta-\sqrt{\delta+\epsilon})^2$, we get from (30) and (2) that

$$\begin{aligned} &\mathrm{P}\Bigg(\exp(nE) \le q_0(L \mid \mathbf{F}) \le \delta^{-2/(k-1)} \times \\ &\qquad \exp\left[n\left(\frac{1}{k-1}D\Big(\mathrm{P}_{Y_1,\dots,Y_k} \| \prod_{i=1}^{k}\mathrm{P}_{Y_i}\Big) + \frac{\delta}{k-1}\right)\right]\Bigg) \\ &\ge (1-\delta-\sqrt{\delta+\epsilon})^2 - \epsilon' > 0, \end{aligned} \tag{31}$$

for all n sufficiently large. It follows that

$$E \le \frac{1}{k-1}D\Big(\mathrm{P}_{Y_1,\dots,Y_k} \| \prod_{i=1}^{k}\mathrm{P}_{Y_i}\Big) + \frac{2\delta}{k-1}.$$

Since E was any ϵ-achievable query exponent and $\delta > 0$ was chosen arbitrarily, the assertion of Theorem 6 is established. □

Proof of Theorem 7: Denote by $\mathcal{L}$ the set of values of the CR L. Using the hypothesis (29) of the theorem, we shall show below the existence of a set $\mathcal{I}_o$ of values of $\mathbf{F}$ and associated sets $\mathcal{L}(\mathbf{i}) \subseteq \mathcal{L}$, $\mathbf{i} \in \mathcal{I}_0$, such that for every $\mathbf{i} \in \mathcal{I}_0$

$$\mathrm{P}_{L|\mathbf{F}}(\mathcal{L}(\mathbf{i}) \mid \mathbf{i}) \ge 1-\delta-\sqrt{\epsilon+\delta}, \tag{32}$$

$$|\mathcal{L}(\mathbf{i})| \le \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}, \tag{33}$$

$$\text{and} \quad \mathrm{P}_{\mathbf{F}}(\mathcal{I}_0) \ge 1-\delta-\sqrt{\epsilon+\delta}. \tag{34}$$

Then, we consider a query strategy q_0 for L given $\mathbf{F}$ as in the proof of converse part of Lemma 3, with L, $\mathbf{F}$, $\mathcal{I}_0$, $\mathcal{L}(\mathbf{i})$ in the roles of U, V, $\mathcal{V}_0$, $\mathcal{U}_v$, respectively. Thus, for all $\mathbf{i} \in \mathcal{I}_0$, $l \in \mathcal{L}(\mathbf{i})$,

$$q_0(l \mid \mathbf{i}) \le |\mathcal{L}(\mathbf{i})| \le \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}},$$

and so, as in (19), we get by (32)–(34)

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \le \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \ge (1-\delta-\sqrt{\delta+\epsilon})^2,$$

thereby establishing the assertion (30).

The existence of the sets $\mathcal{I}_0$ and $\{\mathcal{L}(\mathbf{i}), \mathbf{i} \in \mathcal{I}_0\}$ satisfying (32)–(34) is argued in three steps below.

Step 1: First, we note the following simple property of interactive communication: if rvs $Y_1,\dots,Y_k$ are mutually independent, they remain mutually independent when conditioned on an interactive communication $\mathbf{F}$.

Lemma 8: Let the pmf $\tilde{\mathrm{P}}_{Y_1,\dots,Y_k}$ be such that

$$\tilde{\mathrm{P}}_{Y_1,\dots,Y_k} = \prod_{j=1}^{k}\tilde{\mathrm{P}}_{Y_j}. \tag{35}$$

Then, for $\mathbf{i} = \mathbf{F}(y_1,\dots,y_k)$, we have

$$\tilde{\mathrm{P}}_{Y_1,\dots,Y_k|\mathbf{F}}(y_1,\dots,y_k \mid \mathbf{i}) = \prod_{j=1}^{k}\tilde{\mathrm{P}}_{Y_j|\mathbf{F}}(y_j \mid \mathbf{i}). \tag{36}$$

Proof: The proof follows upon observing that

$$\begin{aligned} &I_{\tilde{\mathrm{P}}}(Y_j \wedge Y_1,\dots,Y_{j-1},Y_{j+1},\dots,Y_k \mid \mathbf{F}) \\ &\le I_{\tilde{\mathrm{P}}}(Y_j \wedge Y_1,\dots,Y_{j-1},Y_{j+1},\dots,Y_k) \\ &= 0, \quad j = 1,\dots,k, \end{aligned} \tag{37}$$

where the first inequality is by [1, Lemma 2.2] upon choosing $U = Y_j$, $V = (Y_1,\dots,Y_{j-1},Y_{j+1},\dots,Y_k)$, Φ to be the communication from terminal j, and Ψ to be the communication from the remaining terminals.

Hereafter in this proof, we shall select

$$\tilde{\mathrm{P}}_{Y_j} = \mathrm{P}_{Y_j}, \quad j = 1,\dots,k. \tag{38}$$

Step 2: In this step, we select the aforementioned set of communication values $\mathcal{I}_0$. Let $L_j = L_j(Y_j,\mathbf{F})$ denote an estimate of CR L at terminal j, $j = 1,\dots,k$ (see Definition 2). Denote by $\mathcal{T}_0$ the set $\{\cdot\}$ on the left-side of (29). For each realization $(l,\mathbf{i})$ of $(L,\mathbf{F})$, denote by $A_{l,\mathbf{i}} \subseteq \mathcal{Y}_1 \times \cdots \times \mathcal{Y}_k$ the set

$$\begin{aligned} A_{l,\mathbf{i}} = \mathcal{T}_0 \cap \{&(y_1,\dots,y_k) : \mathbf{F}(y_1,\dots,y_k) = \mathbf{i}, \\ &L_j(y_j,\mathbf{i}) = L(y_1,\dots,y_k) = l, j = 1,\dots,k\}. \end{aligned} \tag{39}$$

Since L is ϵ-CR from $\mathbf{F}$, we have from (1) and (29) that

$$\mathrm{P}((Y_1,\dots,Y_k) \in A_{L,\mathbf{F}}) \ge 1-\epsilon-\delta.$$

By a reverse Markov inequality, there exists a set $\mathcal{I}_1$ of values of $\mathbf{F}$ with

$$\mathrm{P}_{\mathbf{F}}(\mathcal{I}_1) \ge 1-\sqrt{\epsilon+\delta}, \tag{40}$$

and

$$\mathrm{P}((Y_1,\dots,Y_k) \in A_{L,\mathbf{F}} \mid \mathbf{F} = \mathbf{i}) \ge 1-\sqrt{\epsilon+\delta}, \ \mathbf{i} \in \mathcal{I}_1. \tag{41}$$

Next, denote by $\mathcal{I}_2$ the set of values of $\mathbf{F}$ such that

$$\delta\tilde{\mathrm{P}}_{\mathbf{F}}(\mathbf{i}) \le \mathrm{P}_{\mathbf{F}}(\mathbf{i}), \qquad \mathbf{i} \in \mathcal{I}_2, \tag{42}$$

where $\tilde{\mathrm{P}}_{\mathbf{F}}$ is, as usual, the distribution of $\mathbf{F}$ under $\tilde{\mathrm{P}}$. From Proposition 5 with $Q_1 = \mathrm{P}_{\mathbf{F}}$, $Q_2 = \tilde{\mathrm{P}}_{\mathbf{F}}$, we have

$$\mathrm{P}_{\mathbf{F}}(\mathcal{I}_2) \ge 1-\delta. \tag{43}$$

Thus, by (40) and (43), $\mathcal{I}_0 \triangleq \mathcal{I}_1 \cap \mathcal{I}_2$ satisfies (34).

Step 3: In this step, we identify sets $\mathcal{L}(\mathbf{i})$ that satisfy (32) and (33). For each $\mathbf{i} \in \mathcal{I}_0$, the sets $A_{l,\mathbf{i}}$ corresponding to different values l are disjoint. Upon defining the nonnegative measure[3] μ on $\mathcal{L}$ for each $\mathbf{i} \in \mathcal{I}_0$ by

$$\mu(l) \triangleq \mathrm{P}_{Y_1,\dots,Y_k|\mathbf{F}}(A_{l,\mathbf{i}} \mid \mathbf{i}), \qquad l \in \mathcal{L}, \tag{44}$$

we get

$$\begin{aligned} \mu(\mathcal{L}) &= \sum_{l \in \mathcal{L}} \mathrm{P}_{Y_1,\dots,Y_k|\mathbf{F}}(A_{l,\mathbf{i}} \mid \mathbf{i}) \\ &= \mathrm{P}((Y_1,\dots,Y_k) \in A_{L,\mathbf{i}} \mid \mathbf{F} = \mathbf{i}) \\ &\ge 1-\sqrt{\epsilon+\delta}, \end{aligned}$$

[3] Although μ depends on $\mathbf{i}$, our notation will suppress this dependence.

by (41). Applying Lemma 4 (i) with $\mathcal{L}$ in the role of $\mathcal{U}$, we set $\mathcal{L}(\mathbf{i}) = \mathcal{U}_\delta$, and so

$$\begin{aligned}\mu(\mathcal{L}(\mathbf{i})) &\geq \mu(\mathcal{L}) - \delta \\ &\geq 1 - \delta - \sqrt{\epsilon + \delta}\end{aligned} \tag{45}$$

and

$$|\mathcal{L}(\mathbf{i})| \leq \delta^{-\alpha/(1-\alpha)} \exp\left(H_\alpha(\mu)\right), \quad 0 \leq \alpha < 1. \tag{46}$$

It follows from (45) that

$$\begin{aligned}\mathrm{P}_{L|\mathbf{F}}\left(\mathcal{L}(\mathbf{i}) \mid \mathbf{i}\right) &\geq \sum_{l \in \mathcal{L}(\mathbf{i})} \mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right) \\ &= \mu(\mathcal{L}(\mathbf{i})) \\ &\geq 1 - \delta - \sqrt{\epsilon + \delta},\end{aligned} \tag{47}$$

which establishes (32).

Finally, we obtain an upper bound on $\exp\left(H_\alpha(\mu)\right)$ for $\alpha = \frac{1}{k}$, which will lead to (33). Denote by $A_{l,\mathbf{i}}^j \subseteq \mathcal{Y}_j$ the projection of the set $A_{l,\mathbf{i}} \subseteq \mathcal{Y}_1 \times \cdots \times \mathcal{Y}_k$ along the jth coordinate, $j = 1, \ldots, k$. The sets $A_{l,\mathbf{i}}^j$ are disjoint for different values of l, by definition (see (39)). Thus, for the pmf $\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k}$ in (35), (38), we have

$$\begin{aligned}1 &\geq \prod_{j=1}^k \left[\sum_{l \in \mathcal{L}} \tilde{\mathrm{P}}_{Y_j|\mathbf{F}}\left(A_{l,\mathbf{i}}^j \mid \mathbf{i}\right)\right] \\ &\geq \left[\sum_{l \in \mathcal{L}} \left(\prod_{j=1}^k \tilde{\mathrm{P}}_{Y_j|\mathbf{F}}\left(A_{l,\mathbf{i}}^j \mid \mathbf{i}\right)^{\frac{1}{k}}\right)\right]^k,\end{aligned} \tag{48}$$

where the last step follows from Hölder's inequality[4] [16, Sec. 2.7]. Using (36), the right-side of (48) is the same as

$$\left[\sum_{l \in \mathcal{L}} \tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}}^1 \times \cdots \times A_{l,\mathbf{i}}^k \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k,$$

which is bounded below by

$$\left[\sum_{l \in \mathcal{L}} \tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k, \tag{49}$$

since

$$A_{l,\mathbf{i}} \subseteq A_{l,\mathbf{i}}^1 \times \cdots \times A_{l,\mathbf{i}}^k. \tag{50}$$

Upon noting that $A_{l,\mathbf{i}} \subseteq \mathcal{T}_0$, for all $(y_1, \ldots, y_k) \in A_{l,\mathbf{i}}$, it follows that

$$\begin{aligned}\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(y_1, \ldots, y_k \mid \mathbf{i}\right) &= \frac{\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k}\left(y_1, \ldots, y_k\right)}{\tilde{\mathrm{P}}_{\mathbf{F}}\left(\mathbf{i}\right)} \\ &= \frac{\prod_{j=1}^k \tilde{\mathrm{P}}_{Y_j}\left(y_j\right)}{\tilde{\mathrm{P}}_{\mathbf{F}}\left(\mathbf{i}\right)} \\ &= \frac{\prod_{j=1}^k \mathrm{P}_{Y_j}\left(y_j\right)}{\tilde{\mathrm{P}}_{\mathbf{F}}\left(\mathbf{i}\right)} \\ &\geq \frac{\mathrm{P}_{Y_1,\ldots,Y_k}\left(y_1, \ldots, y_k\right)}{\theta\, \tilde{\mathrm{P}}_{\mathbf{F}}\left(\mathbf{i}\right)} \\ &\geq \frac{\mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(y_1, \ldots, y_k \mid \mathbf{i}\right)}{\delta^{-1}\, \theta},\end{aligned}$$

where the third equality and the subsequent inequalities are by (38), (29), and (42), respectively. Combining the observations above with (48) and (49), we get

$$\begin{aligned}1 &\geq \left[\sum_{l \in \mathcal{L}} \left(\frac{\mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right)}{\delta^{-1}\, \theta}\right)^{\frac{1}{k}}\right]^k, \\ &= \frac{\delta}{\theta}\left[\sum_{l \in \mathcal{L}} \mu(l)^{\frac{1}{k}}\right]^k,\end{aligned}$$

which, recalling Definition 5, further yields

$$\begin{aligned}\exp\left(H_{\frac{1}{k}}(\mu)\right) &= \left[\sum_{l \in \mathcal{L}} \mu(l)^{\frac{1}{k}}\right]^{\frac{k}{k-1}} \\ &\leq \left(\frac{\theta}{\delta}\right)^{\frac{1}{k-1}}.\end{aligned}$$

The previous bound, along with (46), gives (33). □

VI. Converse Proof of Theorem 1 for Arbitrary $\mathcal{A} \subseteq \mathcal{M}$

The converse technique of the previous section for $\mathcal{A} = \mathcal{M}$ can be extended to an arbitrary $\mathcal{A} \subseteq \mathcal{M}$, yielding an analogous upper bound for $E^*(\epsilon)$ in terms of divergences. However, the resulting upper bound is inadequate as it is known to exceed the expression in the right-side of (9) (see [6]). In this section, we develop a new converse technique that targets directly the latter.

The main steps of the general converse proof for the case $\mathcal{A} \subseteq \mathcal{M}$ are analogous to those in the previous section. The central step is the counterpart of Theorem 7, which is given next. Given a fractional partition λ as in (4), its dual partition is $\overline{\lambda} = \overline{\lambda}(\lambda) = \left\{\overline{\lambda}_{B^c}, B \in \mathcal{B}\right\}$ with

$$\overline{\lambda}_{B^c} = \frac{\lambda_B}{\lambda_{\mathtt{sum}} - 1}, \quad B \in \mathcal{B}, \tag{51}$$

[4] See [25, eq. (33)] for an early use of Hölder's inequality in a CR converse proof.

where $\mathcal{B}$ is defined in (3) and $\lambda_{\mathtt{sum}}$ is given by (8). It is known from [20], and can be seen also from (4) and (8), that

$$\begin{aligned}\sum_{B\in\mathcal{B}:B^c\ni i}\overline{\lambda}_{B^c} &= \frac{1}{\lambda_{\mathtt{sum}}-1}\sum_{B\in\mathcal{B}:B^c\ni i}\lambda_B\\ &= \frac{1}{\lambda_{\mathtt{sum}}-1}\left[\sum_{B\in\mathcal{B}}\lambda_B-\sum_{B\in\mathcal{B}:B\ni i}\lambda_B\right]\\ &= \frac{1}{\lambda_{\mathtt{sum}}-1}\left[\lambda_{\mathtt{sum}}-1\right]=1, \quad i\in\mathcal{M}, \quad (52)\end{aligned}$$

so that $\overline{\lambda}$, too, is a fractional partition of $\mathcal{M}$.

Theorem 9: Let $L = L(Y_1,\ldots,Y_m)$ be ϵ-CR for $\mathcal{A}$ from interactive communication $\mathbf{F} = \mathbf{F}(Y_1,\ldots,Y_m)$, $0 < \epsilon < 1$. Given $\delta > 0$ such that $\delta + \sqrt{\delta+\epsilon} < 1$ and a fractional partition $\lambda \in \Lambda(\mathcal{A})$, let θ_{B^c}, $B \in \mathcal{B}$, and θ_0 be such that

$$\mathrm{P}\left(\left\{y_{\mathcal{M}} : \mathrm{P}_{Y_{\mathcal{M}}}(y_{\mathcal{M}}) \le \frac{1}{\theta_0},\ \mathrm{P}_{Y_{B^c}}(y_{B^c}) \ge \frac{1}{\theta_{B^c}}, B\in\mathcal{B}\right\}\right) \ge 1-\delta. \quad (53)$$

Then, with

$$\theta = \frac{\prod_{B\in\mathcal{B}}\theta_{B^c}^{\overline{\lambda}_{B^c}}}{\theta_0}, \quad (54)$$

there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L\mid\mathbf{F}) \le \left(\frac{\theta}{\kappa(\delta)}\right)^{\lambda_{\mathtt{sum}}-1}\right) \ge (1-\delta-\sqrt{\delta+\epsilon})^2, \quad (55)$$

where $\kappa(\delta) = (m2^m)^{-m}\,\delta^{m+1}$.

Proof: As in the proof of Theorem 7, the assertion (55) will follow upon showing the existence of sets $\mathcal{I}_0$ and $\mathcal{L}(\mathbf{i}) \subseteq \mathcal{L}$, $\mathbf{i} \in \mathcal{I}_0$, such that (32) and (34) are satisfied, along with the following replacement for (33):

$$|\mathcal{L}(\mathbf{i})| \le \left(\frac{\theta}{\kappa(\delta)}\right)^{\lambda_{\mathtt{sum}}-1}, \qquad \mathbf{i}\in\mathcal{I}_0. \quad (56)$$

To this end, we provide here appropriate replacements for the three steps in the proof of Theorem 7.

Step 1. For each $B \subsetneq \mathcal{M}$, consider the pmf $\tilde{\mathrm{P}}^B_{Y_{\mathcal{M}}}$ defined by

$$\tilde{\mathrm{P}}^B_{Y_{\mathcal{M}}}(y_{\mathcal{M}}) = \mathrm{P}_{Y_B}(y_B)\,\mathrm{P}_{Y_{B^c}}(y_{B^c}). \quad (57)$$

Note that $\tilde{\mathrm{P}}^B \equiv \tilde{\mathrm{P}}^{B^c}$. The collection of pmfs $\left\{\tilde{\mathrm{P}}^{B^c},\ B\in\mathcal{B}\right\}$ serve as a replacement for the pmf $\tilde{\mathrm{P}}$ in (35).

For the pmf $\tilde{\mathrm{P}}^B$ in (57), we note that

$$I_{\tilde{\mathrm{P}}^B}(Y_B \wedge F_{kj}\mid\Phi_{kj}) = 0, \qquad j\in B^c, \quad (58)$$

since $F_{kj} = f_{kj}(Y_j,\Phi_{kj})$ and Y_{B^c} is independent of Y_B conditioned on Φ_{kj}.

The following lemma serves the role of Lemma 8.

Lemma 10: For $B \subsetneq \mathcal{M}$ and $\mathbf{i} = \mathbf{F}(y_{\mathcal{M}})$, we have

$$\tilde{\mathrm{P}}^B_{Y_B|\mathbf{F}}(y_B\mid\mathbf{i}) = \frac{\mathrm{P}_{Y_B}(y_B)}{\prod_{k=1}^r\prod_{j\in B}\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right)}, \quad (59)$$

where i_{kj}^- denotes the past values of communication in $\mathbf{i}$ for round k and terminal j.

Proof: Note that

$$\begin{aligned}\tilde{\mathrm{P}}^B_{Y_B|\mathbf{F}}(y_B\mid\mathbf{i}) &= \frac{\tilde{\mathrm{P}}^B_{\mathbf{F}|Y_B}(\mathbf{i}\mid y_B)\,\tilde{\mathrm{P}}^B_{Y_B}(y_B)}{\tilde{\mathrm{P}}^B_{\mathbf{F}}(\mathbf{i})}\\ &= \frac{\tilde{\mathrm{P}}^B_{\mathbf{F}|Y_B}(\mathbf{i}\mid y_B)\,\mathrm{P}_{Y_B}(y_B)}{\tilde{\mathrm{P}}^B_{\mathbf{F}}(\mathbf{i})}, \quad (60)\end{aligned}$$

where the previous step is by (57). Furthermore

$$\begin{aligned}\tilde{\mathrm{P}}^B_{\mathbf{F}|Y_B}(\mathbf{i}\mid y_B) &= \prod_{k=1}^r\prod_{j=1}^m\tilde{\mathrm{P}}^B_{F_{kj}|Y_B,\Phi_{kj}}\left(i_{kj}\mid y_B, i_{kj}^-\right)\\ &= \prod_{k=1}^r\prod_{j\in B^c}\tilde{\mathrm{P}}^B_{F_{kj}|Y_B,\Phi_{kj}}\left(i_{kj}\mid y_B, i_{kj}^-\right)\\ &= \prod_{k=1}^r\prod_{j\in B^c}\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right), \quad (61)\end{aligned}$$

where the last step uses (58). Next

$$\begin{aligned}&\tilde{\mathrm{P}}^B_{\mathbf{F}}(\mathbf{i})\\ &= \prod_{k=1}^r\prod_{j=1}^m\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right)\\ &= \prod_{k=1}^r\left(\prod_{j\in B}\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right)\prod_{j\in B^c}\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right)\right).\end{aligned} \quad (62)$$

Then (60), along with (61) and (62), gives (59).

Step 2. Denoting by $\mathcal{T}_0$ the set $\{\cdot\}$ on the left-side of (53), for each $L = l, \mathbf{F} = \mathbf{i}$, define

$$\begin{aligned}A_{l,\mathbf{i}} = \mathcal{T}_0 \cap \{y_{\mathcal{M}} : \mathbf{F}(y_{\mathcal{M}}) = \mathbf{i},&\\ L_j(y_j,\mathbf{i}) = L(y_{\mathcal{M}}) = l, j\in\mathcal{A}\}&. \quad (63)\end{aligned}$$

Analogous to the proof of Theorem 7, the set $\mathcal{I}_1$ of values of $\mathbf{F}$ with

$$\mathrm{P}(Y_{\mathcal{M}} \in A_{L,\mathbf{F}}\mid\mathbf{F}=\mathbf{i}) \ge 1-\sqrt{\epsilon+\delta}, \qquad \mathbf{i}\in\mathcal{I}_1,$$

satisfies

$$\mathrm{P}_{\mathbf{F}}(\mathcal{I}_1) \ge 1-\sqrt{\epsilon+\delta}.$$

For $j \in \mathcal{M}$ and $B \subsetneq \mathcal{M}$, denote by $\mathcal{I}_{j,B}$ the set of $\mathbf{i}$ such that

$$\begin{aligned}&(m2^m)^{-1}\,\delta\prod_{k=1}^r\tilde{\mathrm{P}}^B_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right)\\ &\le \prod_{k=1}^r\mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^-\right). \quad (64)\end{aligned}$$

The following simple extension of Proposition 5 holds:

$$\begin{aligned}
&\mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_{j,B}^c\right)\\
&= \sum_{\mathbf{i}\in\mathcal{I}_{j,B}^c} \mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right)\\
&= \sum_{\mathbf{i}\in\mathcal{I}_{j,B}^c} \prod_{l=1}^{m}\prod_{k=1}^{r} \mathrm{P}_{F_{kl}|\Phi_{kl}}\left(i_{kl}\mid i_{kl}^{-}\right)\\
&= \sum_{\mathbf{i}\in\mathcal{I}_{j,B}^c} \left(\prod_{l\neq j}\prod_{k=1}^{r} \mathrm{P}_{F_{kl}|\Phi_{kl}}\left(i_{kl}\mid i_{kl}^{-}\right)\right)\times\\
&\qquad\qquad \prod_{k=1}^{r} \mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^{-}\right)\\
&< \left(m2^m\right)^{-1}\delta \sum_{\mathbf{i}\in\mathcal{I}_{j,B}^c} \left(\prod_{l\neq j}\prod_{k=1}^{r} \mathrm{P}_{F_{kl}|\Phi_{kl}}\left(i_{kl}\mid i_{kl}^{-}\right)\right)\times\\
&\qquad\qquad \prod_{k=1}^{r} \tilde{\mathrm{P}}_{F_{kj}|\Phi_{kj}}^{B}\left(i_{kj}\mid i_{kj}^{-}\right)\\
&\leq \left(m2^m\right)^{-1}\delta \sum_{\mathbf{i}} \left(\prod_{l\neq j}\prod_{k=1}^{r} \mathrm{P}_{F_{kl}|\Phi_{kl}}\left(i_{kl}\mid i_{kl}^{-}\right)\right)\times\\
&\qquad\qquad \prod_{k=1}^{r} \tilde{\mathrm{P}}_{F_{kj}|\Phi_{kj}}^{B}\left(i_{kj}\mid i_{kj}^{-}\right)\\
&= \left(m2^m\right)^{-1}\delta, \qquad (65)
\end{aligned}$$

where the first inequality is by (64), and (65) holds since the summand is a pmf for $\mathbf{F}$, as can be seen by directly computing the sum. Defining $\mathcal{I}_2 = \bigcap_{j=1}^{m}\bigcap_{B\subsetneq\mathcal{M}} \mathcal{I}_{j,B}$, we get

$$\mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_2\right) \geq 1-\delta.$$

The set $\mathcal{I}_0$ is defined as $\mathcal{I}_1\cap\mathcal{I}_2$, and satisfies (34).

Step 3. Finally, we define sets $\mathcal{L}(\mathbf{i})\subseteq\mathcal{L}$, $\mathbf{i}\in\mathcal{I}_0$ that satisfy (32) and (56). For each $\mathbf{i}\in\mathcal{I}_0$, let

$$\mu(l) = \mathrm{P}_{Y_{\mathcal{M}}|\mathbf{F}}\left(A_{l,\mathbf{i}}\mid\mathbf{i}\right), \qquad l\in\mathcal{L}. \qquad (66)$$

Then, the sets $\mathcal{L}(\mathbf{i})$ satisfying (32) are obtained by an application of Lemma 4 (i) as in (45) and (46) above.

The condition (56) will be obtained upon showing that for

$$\alpha = \frac{\lambda_{\mathtt{sum}}-1}{\lambda_{\mathtt{sum}}}, \qquad (67)$$

it holds that

$$\delta^{-\alpha/(1-\alpha)}\exp\left(H_\alpha(\mu)\right) \leq \left(\frac{\theta}{\kappa(\delta)}\right)^{\lambda_{\mathtt{sum}}-1}. \qquad (68)$$

To do so, first note that for each $B\in\mathcal{B}$, the set $B^c\cap\mathcal{A}$ is nonempty. Thus, by (63), the projections $A_{l,\mathbf{i}}^{B^c}$ of $A_{l,\mathbf{i}}$ along the coordinates in $B^c\subsetneq\mathcal{M}$ are disjoint across $l\in\mathcal{L}$. Thus,

$$1 \geq \prod_{B\in\mathcal{B}}\left(\sum_{l\in\mathcal{L}} \tilde{\mathrm{P}}_{Y_{\mathcal{M}}|\mathbf{F}}^{B^c}\left(A_{l,\mathbf{i}}^{B^c}\mid\mathbf{i}\right)\right)^{\lambda_B}.$$

Using Hölder's inequality [16, Sec. 2.7], and recalling (51) and (8), we get

$$1 \geq \left[\sum_{l\in\mathcal{L}}\left(\prod_{B\in\mathcal{B}} \tilde{\mathrm{P}}_{Y_{\mathcal{M}}|\mathbf{F}}^{B^c}\left(A_{l,\mathbf{i}}^{B^c}\mid\mathbf{i}\right)^{\overline{\lambda}_{B^c}}\right)^{\alpha}\right]^{\frac{1}{1-\alpha}}. \qquad (69)$$

Next, note from Lemma 10 that

$$\tilde{\mathrm{P}}_{Y_{\mathcal{M}}|\mathbf{F}}^{B^c}\left(A_{l,\mathbf{i}}^{B^c}\mid\mathbf{i}\right) = \frac{\sum\limits_{y_{B^c}\in A_{l,\mathbf{i}}^{B^c}} \mathrm{P}_{Y_{B^c}}\left(y_{B^c}\right)}{\prod\limits_{k=1}^{r}\prod\limits_{j\in B^c} \tilde{\mathrm{P}}_{F_{kj}|\Phi_{kj}}^{B^c}\left(i_{kj}\mid i_{kj}^{-}\right)},$$

which, since the order of products can be interchanged, and upon using (64), is bounded below by

$$\frac{\sum\limits_{y_{B^c}\in A_{l,\mathbf{i}}^{B^c}} \mathrm{P}_{Y_{B^c}}\left(y_{B^c}\right)}{\prod\limits_{j\in B^c}\left(m2^m\right)\delta^{-1}\prod\limits_{k=1}^{r}\left[\mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^{-}\right)\right]}.$$

It follows that

$$\begin{aligned}
&\prod_{B\in\mathcal{B}} \tilde{\mathrm{P}}_{Y_{\mathcal{M}}|\mathbf{F}}^{B^c}\left(A_{l,\mathbf{i}}^{B^c}\mid\mathbf{i}\right)^{\overline{\lambda}_{B^c}}\\
&\geq \frac{\prod\limits_{B\in\mathcal{B}}\left[\sum\limits_{y_{B^c}\in A_{l,\mathbf{i}}^{B^c}} \mathrm{P}_{Y_{B^c}}\left(y_{B^c}\right)\right]^{\overline{\lambda}_{B^c}}}{\prod\limits_{B\in\mathcal{B}}\prod\limits_{j\in B^c}\left[\left(m2^m\right)\delta^{-1}\prod\limits_{k=1}^{r}\mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^{-}\right)\right]^{\overline{\lambda}_{B^c}}}.
\end{aligned} \qquad (70)$$

The right-side of (70) can be simplified by noting that

$$\begin{aligned}
&\prod_{B\in\mathcal{B}}\prod_{j\in B^c}\left[\left(m2^m\right)\delta^{-1}\prod_{k=1}^{r}\mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^{-}\right)\right]^{\overline{\lambda}_{B^c}}\\
&= \prod_{j=1}^{m}\left[\left(m2^m\right)\delta^{-1}\prod_{k=1}^{r}\mathrm{P}_{F_{kj}|\Phi_{kj}}\left(i_{kj}\mid i_{kj}^{-}\right)\right]^{\sum_{B\in\mathcal{B}:B^c\ni j}\overline{\lambda}_{B^c}}\\
&= \left(\frac{m2^m}{\delta}\right)^{m}\mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right), \qquad (71)
\end{aligned}$$

where the previous step uses (52). The definition of $\mathcal{T}_0$, along with (70) and (71), gives

$$\begin{aligned}
&\prod_{B\in\mathcal{B}} \tilde{\mathrm{P}}_{Y_{\mathcal{M}}|\mathbf{F}}^{B^c}\left(A_{l,\mathbf{i}}^{B^c}\mid\mathbf{i}\right)^{\overline{\lambda}_{B^c}}\\
&\geq \frac{\delta^m}{\left(m2^m\right)^m\mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right)}\prod_{B\in\mathcal{B}}\left(\frac{\left|A_{l,\mathbf{i}}^{B^c}\right|}{\theta_{B^c}}\right)^{\overline{\lambda}_{B^c}}.
\end{aligned} \qquad (72)$$

Also, since $A_{l,\mathbf{i}}\subseteq\mathcal{T}_0$, we have

$$\mathrm{P}_{Y_{\mathcal{M}}}\left(A_{l,\mathbf{i}}\right) \leq \frac{\left|A_{l,\mathbf{i}}\right|}{\theta_0},$$

which, with (54) and (72), gives

$$\prod_{B\in\mathcal{B}} \tilde{\mathrm{P}}^{B^c}_{Y_{\mathcal{M}}|\mathbf{F}}\left(A^{B^c}_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\overline{\lambda}_{B^c}} \geq \frac{\delta^m}{(m2^m)^m\,\theta}\left(\frac{\prod_{B\in\mathcal{B}}\left|A^{B^c}_{l,\mathbf{i}}\right|^{\overline{\lambda}_{B^c}}}{\left|A_{l,\mathbf{i}}\right|}\right)\mathrm{P}_{Y_{\mathcal{M}}|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right). \tag{73}$$

Since $\overline{\lambda}$ is a fractional partition, [19, Corollary 3.4] implies

$$\left(\frac{\prod_{B\in\mathcal{B}}\left|A^{B^c}_{l,\mathbf{i}}\right|^{\overline{\lambda}_{B^c}}}{\left|A_{l,\mathbf{i}}\right|}\right) \geq 1, \tag{74}$$

which combined with (69)–(74) yields

$$1 \geq \left(\frac{\delta^m}{(m2^m)^m\,\theta}\right)^{\frac{\alpha}{1-\alpha}}\left[\sum_{l\in\mathcal{L}}\mu(l)^{\alpha}\right]^{\frac{1}{1-\alpha}}.$$

The previous inequality implies (68) since

$$\frac{\alpha}{1-\alpha} = \lambda_{\mathtt{sum}} - 1.$$

□

VII. Strong Converse for SK Capacity

A byproduct of Theorem 1 is a new result that establishes a strong converse for the SK capacity of a multiterminal source model, for the terminals in $\mathcal{A} \subseteq \mathcal{M}$. In this context, we shall consider –without loss of effect– a weaker notion of security index than in (7), defined in terms of variational distance:

$$s_{var}(K;\mathbf{F}) = \sum_{\mathbf{i}} \mathrm{P}_{\mathbf{F}}(\mathbf{i}) \sum_{k=1}^{\|K\|}\left|\mathrm{P}_{K|\mathbf{F}}(k \mid \mathbf{i}) - \frac{1}{\|K\|}\right|. \tag{75}$$

However, the requirement (6) on s_{in} will be replaced now by

$$\lim_n n s_{\mathrm{var}}(K;\mathbf{F}) = 0. \tag{76}$$

Definition 6: Given $0<\epsilon<1$, $R \geq 0$ is an ϵ-achievable SK rate for $\mathcal{A} \subseteq \mathcal{M}$ if for every $\rho > 0$, there is an $N = N(\epsilon,\rho)$ such that for every $n \geq N$, there exists an ϵ-CR $K = K\left(X^n_{\mathcal{M}}\right)$ for $\mathcal{A}$ from $\mathbf{F}$ satisfying

$$\frac{1}{n}\log\|K\| \geq R - \rho, \tag{77}$$

and

$$s_{\mathrm{var}}(K;\mathbf{F}) \leq \frac{\rho}{n}. \tag{78}$$

The supremum of ϵ-achievable SK rates is the ϵ-SK capacity, denoted $C(\epsilon)$. The SK capacity is the infimum of $C(\epsilon)$ for $0 < \epsilon < 1$. We recall the following.

Theorem 11: [9] The SK capacity for $\mathcal{A} \subseteq \mathcal{M}$ is

$$C = E^* = H\left(X_{\mathcal{M}}\right) - \max_{\lambda\in\Lambda(\mathcal{A})}\sum_{B\in\mathcal{B}}\lambda_B H\left(X_B \mid X_{B^c}\right), \quad 0<\epsilon<1.$$

Remark: The (new) secrecy requirement (76) is not unduly restrictive. Indeed, the achievability proof of Theorem 11 [9] holds with $s_{in}(K;\mathbf{F})$ vanishing to zero exponentially rapidly in n, which, by Pinsker's inequality (cf., [11]), implies (76). The converse proof in [9] was shown under the "weak secrecy" condition

$$\lim_n \frac{1}{n} I(K \wedge \mathbf{F}) = 0, \tag{79}$$

which, in turn, is implied by (76) by a simple application of [9, Lemma 1].

The strong converse for SK capacity, valid under (76), is given next.

Theorem 12: For every $0<\epsilon<1$, it holds that

$$C(\epsilon) = C. \tag{80}$$

Remark: It is not known if the strong converse in Theorem 12 holds under (79).

Proof: Theorem 11 [9] already provides the proof of achievability, i.e., $C(\epsilon) \geq C$. The converse proof below shows that if R is an ϵ-achievable SK rate, then R is an ϵ-achievable query exponent. Therefore

$$R \leq E^*(\epsilon) = C, \quad 0<\epsilon<1, \tag{81}$$

where the equality is by (5). Specifically, for every $\rho > 0$, suppose that there exists $K = K\left(X^n_{\mathcal{M}}\right)$ and communication $\mathbf{F}$ satisfying (77) and (78) for all n sufficiently large. We claim that the hypothesis (11) of Lemma 3 holds with $U = K$, $V = \mathbf{F}$, and $\gamma = \exp[n(R-2\rho)]$ for every $0<\delta<1/2$, when ρ is sufficiently small. Therefore, by (12), $R - 2\rho$ is an ϵ-achievable query exponent which leads to (81) since ρ can be chosen arbitrarily small.

Turning to the claim, observe that

$$\begin{aligned}
&\mathrm{P}\left(\left\{(k,\mathbf{i}) : \mathrm{P}_{K|\mathbf{F}}(k \mid \mathbf{i}) > \frac{2}{\exp[n(R-\rho)]}\right\}\right) \\
&\leq \mathrm{P}\left(\left\{(k,\mathbf{i}) : \mathrm{P}_{K|\mathbf{F}}(k \mid \mathbf{i}) > \frac{2}{\|K\|}\right\}\right) \\
&\leq \mathrm{P}\left(\left\{(k,\mathbf{i}) : \left|\log\|K\|\mathrm{P}_{K|\mathbf{F}}(k \mid \mathbf{i})\right| > 1\right\}\right) \\
&\leq \mathbb{E}\left[\left|\log\|K\|\mathrm{P}_{K|\mathbf{F}}(K \mid \mathbf{F})\right|\right],
\end{aligned}$$

where the first and the last inequality above follow from (77) and the Markov inequality, respectively.

Next, we show that

$$\mathbb{E}\left[\left|\log\|K\|\mathrm{P}_{K|\mathbf{F}}(K \mid \mathbf{F})\right|\right] \leq s_{\mathrm{var}}(K;\mathbf{F})\log\frac{\|K\|^2}{s_{\mathrm{var}}(K;\mathbf{F})}. \tag{82}$$

Then, the right-side can be bounded above by

$$\frac{\rho}{n}\log\frac{n}{\rho} + 2\rho\log\left|X_{\mathcal{M}}\right|, \tag{83}$$

for all n sufficiently large; the claim follows upon taking $n \to \infty$ and $\rho \to 0$. To see (82), note that for $t_1, t_2,\ |t_1 - t_2| < 1$, $f(t) \triangleq -t \log t$ satisfies (cf., [11, Lemma 2.7])

$$\big|f(t_1) - f(t_2)\big| \leq \big|t_1 - t_2\big| \log \frac{1}{\big|t_1 - t_2\big|}. \tag{84}$$

Then, for $\mathbf{F} = \mathbf{i}$

$$\begin{aligned}
&\sum_k \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) \big|\log \|K\| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right)\big| \\
&= \sum_k \Bigg| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) \log \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) + \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) \log \|K\| \\
&\qquad\qquad + \frac{1}{\|K\|} \log \|K\| - \frac{1}{\|K\|} \log \|K\| \Bigg| \\
&\leq \sum_k \Bigg[\bigg| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) \log \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) - \frac{1}{\|K\|} \log \frac{1}{\|K\|} \bigg| \\
&\qquad\qquad + \bigg| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) - \frac{1}{\|K\|} \bigg| \log \|K\| \Bigg] \\
&\leq \sum_k \bigg| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) - \frac{1}{\|K\|} \bigg| \log \frac{\|K\|}{\Big| \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right) - \frac{1}{\|K\|} \Big|}, \qquad (85)
\end{aligned}$$

where the previous inequality uses (84) with $t_1 = \mathrm{P}_{K|\mathbf{F}}\left(k \mid \mathbf{i}\right)$ and $t_2 = \|K\|^{-1}$ for every value k of K. Finally, (82) follows upon multiplying both sides by $\mathrm{P}_{\mathbf{F}}\left(\mathbf{i}\right)$, summing over $\mathbf{i}$, and using the log-sum inequality [11]. □

Observe that the proof of Theorem 12 does not rely on the form of the rvs $K, \mathbf{F}$, and is, in effect, a statement relating the *size* of any achievable SK rate under the s_{var}-secrecy requirement (76) to the query exponent. As a consequence, also the SK capacity for more complex models in which the eavesdropper has additional access to side information can be bounded above by the optimum query exponent when the querier, too, is given access to the same side information.

VIII. General Alphabet Converse for $\mathcal{A} = \mathcal{M}$

In this section, we present a converse technique for the optimum query exponent for rvs with general alphabets, with jointly Gaussian rvs as a special case. No corresponding general claim is made regarding achievability of the exponent. Our technique also leads to a new strong converse for Gaussian SK capacity [22].

Let $\mathcal{Y}_i$ be a complete separable metric space, with associated Borel σ-field σ_i, $1 \leq i \leq k$; a special case of interest is $\mathcal{Y}_i = \mathbb{R}^{n_i}$. Denote by $\mathcal{Y}^k$ the set $\mathcal{Y}_1 \times \cdots \times \mathcal{Y}_k$ and by σ^k the product σ-field[5] $\sigma_1 \times \cdots \times \sigma_k$ on $\mathcal{Y}^k$. Let $\mathrm{P} = \mathrm{P}_{Y_1,\ldots,Y_k}$ be a probability measure on $\left(\mathcal{Y}^k, \sigma^k\right)$. The interactive communication $\{F_{ji} : 1 \leq j \leq r, 1 \leq i \leq k\}$ is specified as in Definition 1, with the rv F_{ji} taking values in, say, $(\mathcal{Z}_{ji}, \mathcal{F}_{ji})$, and being σ_i-measurable for each fixed value of the preceding communication

$$\Phi_{ji} = \left(F_{st} : 1 \leq s < j, 1 \leq t \leq k \text{ or } s = j, 1 \leq t < i\right).$$

Then, there exists a unique regular conditional probability measure on $\left(\mathcal{Y}^k, \sigma^k\right)$ conditioned on $\sigma(\mathbf{F})$, denoted $\mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}$ (cf., [4, Ch. 6]). The notation $Q_{\mathbf{i}}$ will be used interchangeably for the probability measure $\mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(\cdot \mid \mathbf{i}\right)$. We make the following basic assumption of absolute continuity:

$$Q_{\mathbf{i}} \ll \mathrm{P}_{Y_1,\ldots,Y_k}, \qquad \mathrm{P}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}, \tag{86}$$

i.e., (86) holds over a set of $\mathbf{i}$ with $\mathrm{P}_{\mathbf{F}}$-probability 1. Assumption (86) is satisfied by a large class of interactive communication protocols including $\mathbf{F}$ taking countably many values. Moreover, we can assume the following without loss of generality:

$$Q_{\mathbf{i}}\left(\mathbf{F}^{-1}(\mathbf{i})^c\right) = 0, \qquad \mathrm{P}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}, \tag{87}$$

$$\frac{d\,Q_{\mathbf{i}}}{d\,\mathrm{P}}(y^k) = 0, \quad \text{for } y^k \in \mathbf{F}^{-1}(\mathbf{i})^c,\ \mathrm{P}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}. \tag{88}$$

Next, we define ϵ-CR L from $\mathbf{F}$ and its local estimates L_i, respectively, as rvs *taking countably many values*, measurable with respect to σ^k and $\sigma_i \times \sigma(\mathbf{F})$, $1 \leq i \leq k$, and satisfying

$$\mathrm{P}\left(L = L_i,\ 1 \leq i \leq k\right) \geq 1 - \epsilon.$$

The main result of this section, given below, extends Theorem 7 to general measures as above.

Theorem 13: For $0 < \epsilon < 1$, let L be ϵ-CR from interactive communication $\mathbf{F}$. Let $\tilde{\mathrm{P}} = \tilde{\mathrm{P}}_{Y_1,\ldots,Y_k}$ be a probability measure on $\left(\mathcal{Y}^k, \sigma^k\right)$ with

$$\tilde{\mathrm{P}}\left(A_1 \times \cdots \times A_k\right) = \prod_{i=1}^{k} \mathrm{P}_{Y_i}\left(A_i\right) \qquad A_i \in \sigma_i,\ 1 \leq i \leq k. \tag{89}$$

Assuming that $\mathrm{P} \ll \tilde{\mathrm{P}}$, and given $\delta > 0$ such that $\delta + \sqrt{\delta + \epsilon} < 1$, let θ be such that

$$\mathrm{P}\left(\left\{y^k : \frac{d\,\mathrm{P}}{d\,\tilde{\mathrm{P}}}(y^k) \leq \theta\right\}\right) \geq 1 - \delta. \tag{90}$$

Then, there exists a query strategy q_0 for L given $\mathbf{F}$ such that

$$\mathrm{P}\left(q_0(L \mid \mathbf{F}) \leq \left(\frac{\theta}{\delta^2}\right)^{\frac{1}{k-1}}\right) \geq (1 - \delta - \sqrt{\delta + \epsilon})^2. \tag{91}$$

The proof of Theorem 13 is deferred to the end of this section. At this point, we present its implications for a Gaussian setup. Let $X_i^{(n)}$ be an $\mathbb{R}^n$-valued rv, $i = 1, \ldots, m$, and let $X_{\mathcal{M}}^{(n)} = \left(X_1^{(n)}, \ldots, X_m^{(n)}\right)$ be jointly Gaussian $\mathcal{N}(\mathbf{0}, \Sigma^{(n)})$, where $\Sigma^{(n)}$ is a positive-definite matrix. We remark that $X_{\mathcal{M}}^{(n)}$ need not be independent or identically distributed across n. The notion of an ϵ-optimum query exponent $E^*(\epsilon)$, $0 < \epsilon < 1$, is exactly as in Definition 4, even though the underlying CR now can take countably many values. Also, given a partition π of $\mathcal{M}$ with $|\pi| = k$, $2 \leq k \leq m$, the quantity $E_\pi^*(\epsilon)$ is defined as in Section V.

[5] Hereafter, the term "product σ-field" of σ-fields $\sigma_1, \ldots, \sigma_k$, will mean the smallest σ-field containing sets from $\sigma_1 \times \cdots \times \sigma_k$, and will be denoted, with an abuse of notation, simply as $\sigma^k = \sigma_1 \times \cdots \times \sigma_k$.

Proposition 14: For $X_{\mathcal{M}}^{(n)} \sim \mathcal{N}(\mathbf{0}, \Sigma^{(n)})$ with $\Sigma^{(n)}$ being positive definite, it holds that

$$E^*(\epsilon) \leq \min_{\pi} E^*_{\pi}(\epsilon)$$
$$\leq \min_{\pi} \frac{1}{2(|\pi|-1)} \limsup_{n} \frac{1}{n} \log \frac{\prod_{i=1}^{|\pi|} |\Sigma_{\pi_i}^{(n)}|}{|\Sigma^{(n)}|}, \quad 0 < \epsilon < 1,$$

where $\Sigma_{\pi_i}^{(n)}$ is the covariance matrix of $X_{\pi_i}^{(n)}$, $i = 1, \ldots, |\pi|$, and $| \cdot |$ denotes determinant.

Corollary: When $X_{\mathcal{M}}^{(n)}$ is i.i.d. in n with $X_{\mathcal{M}} \sim \mathcal{N}(\mathbf{0}, \Sigma)$

$$E^*(\epsilon) \leq \min_{\pi} \frac{1}{2(|\pi|-1)} \log \frac{\prod_{i=1}^{|\pi|} |\Sigma_{\pi_i}|}{|\Sigma|}, \quad 0 < \epsilon < 1.$$

Proof: Proceeding as in the proof of Theorem 6, we apply Theorem 13 to the rvs $Y_i = X_{\pi_i}^{(n)}$, $1 \leq i \leq |\pi|$. Specifically, we show that the hypothesis (90) is satisfied with

$$\theta = \theta_n = \left(\frac{\prod_{i=1}^{|\pi|} |\Sigma_{\pi_i}^{n}|}{|\Sigma^{(n)}|} \right)^{1/2} \exp(n\delta), \tag{92}$$

where $0 < \delta < 1/2$ is arbitrary. Then, the Proposition follows from the definition of $E^*(\epsilon)$ and (92) as in the proof of Theorem 6. The Corollary results by a straightforward calculation. It remains to verify that (90) holds for θ in (92). For $B \subsetneq \mathcal{M}, B \neq \emptyset$, let g_B denote the density of the Gaussian rv $X_B^{(n)}$. From the AEP for Gaussian rvs [8, equation (47)] (see also [5])

$$\mathrm{P}\left(\left| -\frac{1}{n} \log g_B\left(X_B^{(n)}\right) - \frac{1}{n} h\left(X_B^{(n)}\right) \right| > \tau, \right.$$
$$\left. \text{for some } \emptyset \neq B \subseteq \mathcal{M} \right)$$
$$< 2^m \exp(-c(\tau) n), \quad \tau > 0, \tag{93}$$

where h denotes differential entropy and $c(\tau) > 0$ is a positive constant that does not depend on n. Since

$$\frac{d\mathrm{P}}{d\tilde{\mathrm{P}}} = \frac{g_{\mathcal{M}}}{\prod_{i=1}^{|\pi|} g_{\pi_i}}, \qquad \mathrm{P} \text{ a.s}$$

and

$$h\left(X_{\mathcal{M}}^{(n)}\right) = \frac{1}{2} \log(2\pi e)^{mn} |\Sigma^{(n)}|,$$
$$h\left(X_{\pi_i}^{(n)}\right) = \frac{1}{2} \log(2\pi e)^{|\pi_i| n} |\Sigma_{\pi_i}^{(n)}|, \qquad 1 \leq i \leq |\pi|,$$

using the upper and lower bounds from (93) that hold with significant probability for all n sufficiently large, we get that (90) holds with θ as in (92), for $0 < \delta < 1/2$. □

As an application of the Corollary above, we establish a new strong converse for SK capacity when the underlying rvs $X_{\mathcal{M}}^{(n)}$ are i.i.d. Gaussian in n; for this model, the SK capacity was established in [22]. The notions of ϵ-achievable SK rate, ϵ-SK capacity $C(\epsilon)$, and SK capacity C are as in Definition 6, with condition (77) replaced by

$$\texttt{range}(K) = \{1, \ldots, \lfloor \exp(nR) \rfloor\}, \tag{94}$$

which rules out such rvs K as take infinitely many values.

Proposition 15: When $X_{\mathcal{M}}^{(n)}$ is i.i.d. in n with $X_{\mathcal{M}} \sim \mathcal{N}(\mathbf{0}, \Sigma)$,

$$C(\epsilon) = \min_{\pi} \frac{1}{2(|\pi|-1)} \log \frac{\prod_{i=1}^{|\pi|} |\Sigma_{\pi_i}|}{|\Sigma|}, \quad 0 < \epsilon < 1. \tag{95}$$

Proof: That $C(\epsilon)$ is no smaller than the right-side of (95) follows from the achievability proof in [22].

The proof of the reverse inequality is along the lines of the proof of Theorem 12 and is obtained upon replacing the upper bound (83) by

$$\frac{\rho}{n} \log \frac{n}{\rho} + 2\rho R,$$

and noting that Lemma 3 can be extended straightforwardly to an arbitrary rv V (with the explicit summations in the proof of that lemma written as expectations), provided that the rv U is finite-valued. □

Proof of Theorem 13: In the manner of the proof of Theorem 7, it suffices to identify measurable sets $\mathcal{I}_0$ and $\mathcal{L}(\mathbf{i}) \subseteq \mathcal{L}$, $\mathbf{i} \in \mathcal{I}_0$, such that (32)–(34) are satisfied. In the following, we generalize appropriately the steps 1–3 in the proof of Theorem 7.

Step 1. The following claim is an extension of Lemma 8.

Lemma 16: Given measurable sets $A_i \in \sigma_i$, $1 \leq i \leq k$, for $\tilde{\mathrm{P}}$ in (89)

$$\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_1 \times \cdots \times A_k \mid \mathbf{i}\right) = \prod_{j=1}^{k} \tilde{\mathrm{P}}_{Y_j|\mathbf{F}}\left(A_j \mid \mathbf{i}\right),$$
$$\mathrm{P}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}, \tag{96}$$

where $\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}$ is the regular conditional probability on $(\mathcal{Y}^k, \sigma^k)$ conditioned on $\sigma(\mathbf{F})$.

The proof uses the interactive property of the communication and is relegated to the Appendix.

Step 2. Next, we identify the set $\mathcal{I}_0$. The following technical observation will be used.

Lemma 17: For every $A_0 \in \sigma^k$ such that

$$\frac{d\mathrm{P}}{d\tilde{\mathrm{P}}}(y^k) > 0, \qquad y^k \in A_0, \tag{97}$$

it holds that

$$\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_0 \mid \mathbf{i}\right) = \frac{d\mathrm{P}_{\mathbf{F}}}{d\tilde{\mathrm{P}}_{\mathbf{F}}}(\mathbf{i}) \int_{A_0} \frac{dQ_{\mathbf{i}}}{d\mathrm{P}}\, d\tilde{\mathrm{P}}, \quad \tilde{\mathrm{P}}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}. \tag{98}$$

The proof is given in the Appendix. Denoting by $\mathcal{T}_0$ the set $\left\{y^k \in \mathcal{Y}^k : 0 < \frac{d\mathrm{P}}{d\tilde{\mathrm{P}}}(y^k) \leq \theta\right\}$, let

$$A_l = \mathcal{T}_0 \cap \left\{y^k : L_j\big(y_j, \mathbf{F}(y^k)\big) = L(y^k) = l, 1 \leq j \leq k\right\},$$
$$l \in \mathcal{L}.$$

Then, for $A_{l,\mathbf{i}} \triangleq A_l \cap \mathbf{F}^{-1}(\mathbf{i})$, (87), (88), and Lemma 17 imply

$$\tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right) = \frac{d\mathrm{P}_{\mathbf{F}}}{d\tilde{\mathrm{P}}_{\mathbf{F}}}(\mathbf{i}) \int_{A_{l,\mathbf{i}}} \frac{dQ_{\mathbf{i}}}{d\mathrm{P}}\, d\tilde{\mathrm{P}}, \quad \tilde{\mathrm{P}}_{\mathbf{F}} \text{ a.s. in } \mathbf{i}. \tag{99}$$

In the following, we restrict attention to the set of values of $\mathbf{F}$ for which (99) holds for every $l \in \mathcal{L}$; this set has $\tilde{\mathrm{P}}_{\mathbf{F}}$ measure 1 by (98) since the set $\mathcal{L}$ is countable. Proceeding along the lines of the proof of Theorem 7, we define $\mathcal{I}_1$ as the set of those $\mathbf{i}$ for which

$$\mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right) \geq 1 - \sqrt{\epsilon + \delta}. \tag{100}$$

Since L is an ϵ-CR from $\mathbf{F}$, it follows from (90), the fact that

$$\mathrm{P}\left(\left\{y^k : \frac{d\,\mathrm{P}}{d\,\tilde{\mathrm{P}}}(y^k) = 0\right\}\right) = 0,$$

and by a reverse Markov inequality, that

$$\mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_1\right) \geq 1 - \sqrt{\epsilon + \delta}. \tag{101}$$

Furthermore, for the set $\mathcal{I}_2$ of values $\mathbf{i}$ of $\mathbf{F}$ satisfying

$$\frac{d\,\mathrm{P}_{\mathbf{F}}}{d\,\tilde{\mathrm{P}}_{\mathbf{F}}}(\mathbf{i}) \geq \delta, \tag{102}$$

it holds that

$$\mathrm{P}_{\mathbf{F}}\left(\mathcal{I}_2\right) \geq 1 - \delta, \tag{103}$$

since

$$\begin{aligned}\int_{\mathcal{I}_2^c} d\,\mathrm{P}_{\mathbf{F}} &= \int_{\mathcal{I}_2^c} \frac{d\,\mathrm{P}_{\mathbf{F}}}{d\,\tilde{\mathrm{P}}_{\mathbf{F}}} d\,\tilde{\mathrm{P}}_{\mathbf{F}} \\ &< \delta.\end{aligned}$$

Define $\mathcal{I}_0 = \mathcal{I}_1 \cap \mathcal{I}_2$; (34) follows from (101) and (103).

Step 3. Since Lemma 4 (i) applies to a countable set $\mathcal{U} = \mathcal{L}$, defining the nonnegative measure μ on $\mathcal{L}$ as in (44) for each $\mathbf{i} \in \mathcal{I}_0$ and using (100), the sets $\mathcal{L}(\mathbf{i})$ obtained in (45)–(47) satisfy (32). Also, condition (33) will follow from (46) upon showing that

$$\exp\left(H_\alpha(\mu)\right) \leq \left(\frac{\theta}{\delta}\right)^{\frac{1}{k-1}}. \tag{104}$$

To do so, denote by $A^j_{l,\mathbf{i}}$ the projection of $A_{l,\mathbf{i}}$ along the jth coordinate, $1 \leq j \leq k$. As before, the sets $A^j_{l,\mathbf{i}}$ are disjoint across $l \in \mathcal{L}$. Then, Hölder's inequality [16] implies that

$$\begin{aligned}1 &\geq \prod_{j=1}^{k}\left[\sum_{l\in\mathcal{L}} \tilde{\mathrm{P}}_{Y_j|\mathbf{F}}\left(A^j_{l,\mathbf{i}} \mid \mathbf{i}\right)\right] \\ &\geq \left[\sum_{l\in\mathcal{L}}\left(\prod_{j=1}^{k} \tilde{\mathrm{P}}_{Y_j|\mathbf{F}}\left(A^j_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right)\right]^k \\ &= \left[\sum_{l\in\mathcal{L}} \tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A^1_{l,\mathbf{i}} \times \cdots \times A^k_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k, \end{aligned} \tag{105}$$

where the previous step uses Lemma 16. The right-side of (105) is bounded below by

$$\left[\sum_{l\in\mathcal{L}} \tilde{\mathrm{P}}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k,$$

since $A_{l,\mathbf{i}} \subseteq A^1_{l,\mathbf{i}} \times \cdots \times A^k_{l,\mathbf{i}}$, which by (99) equals

$$\left[\sum_{l\in\mathcal{L}}\left(\frac{d\,\mathrm{P}_{\mathbf{F}}}{d\,\tilde{\mathrm{P}}_{\mathbf{F}}}(\mathbf{i}) \int_{A_{l,\mathbf{i}}} \frac{d\,Q_{\mathbf{i}}}{d\,\mathrm{P}} d\,\tilde{\mathrm{P}}\right)^{\frac{1}{k}}\right]^k.$$

From the definition of the set $\mathcal{I}_2$ in (102), the expression above exceeds

$$\left[\sum_{l\in\mathcal{L}}\left(\delta \int_{A_{l,\mathbf{i}}} \frac{d\,Q_{\mathbf{i}}}{d\,\mathrm{P}} d\,\tilde{\mathrm{P}}\right)^{\frac{1}{k}}\right]^k,$$

which is the same as

$$\left[\sum_{l\in\mathcal{L}}\left(\delta \int_{A_{l,\mathbf{i}}} \frac{d\,Q_{\mathbf{i}}}{d\,\mathrm{P}} \frac{d\,\mathrm{P}/d\,\tilde{\mathrm{P}}}{d\,\mathrm{P}/d\,\tilde{\mathrm{P}}} d\,\tilde{\mathrm{P}}\right)^{\frac{1}{k}}\right]^k. \tag{106}$$

Since $A_{l,\mathbf{i}} \subseteq \mathcal{T}_0$, the sum in (106) is bounded below further by

$$\begin{aligned}&\left[\sum_{l\in\mathcal{L}}\left(\frac{\delta}{\theta} \int_{A_{l,\mathbf{i}}} \frac{d\,Q_{\mathbf{i}}}{d\,\mathrm{P}} \frac{d\,\mathrm{P}}{d\,\tilde{\mathrm{P}}} d\,\tilde{\mathrm{P}}\right)^{\frac{1}{k}}\right]^k \\ &= \frac{\delta}{\theta}\left[\sum_{l\in\mathcal{L}}\left(\int_{A_{l,\mathbf{i}}} d\,Q_{\mathbf{i}}\right)^{\frac{1}{k}}\right]^k \\ &= \frac{\delta}{\theta}\left[\sum_{l\in\mathcal{L}} \mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k.\end{aligned}$$

Combining the observations above from (105) onward, we have

$$\frac{\theta}{\delta} \geq \left[\sum_{l\in\mathcal{L}} \mathrm{P}_{Y_1,\ldots,Y_k|\mathbf{F}}\left(A_{l,\mathbf{i}} \mid \mathbf{i}\right)^{\frac{1}{k}}\right]^k,$$

which is the same as (104) with $\alpha = 1/k$. □

IX. Discussion

A. General Lossless Source Coding Theorem

Our Lemma 4 relating the cardinalities of large probability sets to Rényi entropy played a material role in the converse proofs. It is also of independent interest, and can be interpreted as a source coding result for a general source with finite alphabet $\mathcal{U}$. Furthermore, it leads to the following asymptotic result.

Consider a sequence of probability measures μ_n on finite sets $\mathcal{U}_n$, $n \geq 1$. For $0 < \delta < 1$, R is a δ-achievable (block) source coding rate if there exists sets $\mathcal{V}_n \subseteq \mathcal{U}_n$ satisfying

$$\mu_n(\mathcal{V}_n) \geq 1 - \delta,$$

for all n sufficiently large, and

$$\limsup_n \frac{1}{n} \log|\mathcal{V}_n| \leq R.$$

The optimum source coding rate $R^*(\delta)$ is the infimum of all such δ-achievable rates.

Proposition 18: For each $0 < \delta < 1$

$$\lim_{\alpha\downarrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n) \le R^*(\delta) \le \lim_{\alpha\uparrow 1} \limsup_n \frac{1}{n} H_\alpha(\mu_n). \tag{107}$$

Corollary: If μ_n is an i.i.d. probability measure on $\mathcal{U}_n = \mathcal{U} \times \cdots \times \mathcal{U}$, then

$$R^*(\delta) = H(\mu_1), \qquad 0 < \delta < 1.$$

Proof: The Proposition is a direct consequence of Lemma 4 upon taking appropriate limits in (21) and (22) with $\mathcal{U}_n$ in the role of $\mathcal{U}$. The Corollary follows since for i.i.d. μ_n

$$H_\alpha(\mu_n) = nH_\alpha(\mu_1) \text{ and } \lim_{\alpha\to 1} H_\alpha(\mu_1) = H(\mu_1).$$

□

Note that the above Corollary is proved without recourse to the AEP. Moreover, it contains a strong converse for the lossless coding theorem for an i.i.d. source. In general, Proposition 18 implies a strong converse whenever the lower and upper bounds for $R^*(\delta)$ in (107) coincide. This implication is a special case of a general source coding result in [13, Th. 1.5.1], [15], where it was shown that a strong converse holds iff for rvs U_n with pmfs μ_n, the "lim-inf" and "lim-sup" of $Z_n = \frac{1}{n}\log\frac{1}{\mu_n(U_n)}$ in μ_n-probability coincide, i.e.,

$$\begin{aligned} &\sup\left\{\beta : \lim_n \mu_n(Z_n < \beta) = 0\right\} \\ &= \inf\left\{\beta : \lim_n \mu_n(Z_n > \beta) = 0\right\}. \end{aligned} \tag{108}$$

In fact, a straightforward calculation shows that the lower and upper bounds for $R^*(\delta)$ in (107) are admissible choices of β on the left- and right-sides of (108), respectively.

B. General Models

The description of the optimum query exponent in Definition 4 can be refined to display an explicit dependence on ϵ'. Let $E^*(\epsilon, \epsilon')$ denote the optimum query exponent for fixed $0 < \epsilon, \epsilon' < 1$. Our proofs establish $E^*(\epsilon, \epsilon')$ equals the right-side of (5) for $\epsilon' < (1 - \sqrt{\epsilon})^2$ (see (31)). For $\epsilon' > 1 - \epsilon$, as suggested by a reviewer, the following construction of L renders $E^*(\epsilon, \epsilon')$ unbounded: Choose $L = 0$ with probability $(1 - \epsilon)$ and uniformly distributed on a sufficiently large set with probability ϵ. For the remaining values of ϵ, ϵ', $E^*(\epsilon, \epsilon')$ is not known.

A less restrictive model for querying than that in Section II can be considered, allowing general queries with binary answers. Such a query strategy can be represented as a search on a binary tree whose leaves correspond to the values of the CR L. The query strategies considered in this paper correspond to the case where the search tree is a path with leaves attached to each node. For a general tree model, our results can be adapted to show that the maximum number of queries that can be inflicted on a querier grows only linearly in n at a rate that is equal to the expression for E^* in (5).

We remark also that allowing randomness at the terminals in $\mathcal{M}$ for interactive communication and CR recovery does not improve the optimum query exponent. Such randomization is described by mutually independent rvs $W_1, \ldots, W_m$, where each W_i is distributed uniformly on the (finite) set $\{1, \ldots, w_i\}$, and the rvs $W_1, \ldots, W_m$ are independent of $X^n_{\mathcal{M}}$. The claim of the remark is seen from the converse result in Theorem 9. Indeed, the assertion (55) of Theorem 9 remains unchanged upon replacing Y_i by (Y_i, W_i), $i \in \mathcal{M}$, θ_0 by $\theta_0\left(\prod_{i\in\mathcal{M}} w_i\right)$, and θ_{B^c} by $\theta_{B^c}\left(\prod_{i\in B^c} w_i\right)$, $B \in \mathcal{B}$; and observing that in (54), the w_i-terms cancel in the numerator and the denominator.

Finally, Lemma 3, which considered rvs U, V, can be used to characterize the optimum query exponent Γ^* for a family of finite-valued rvs $\{U_n, V_n\}_{n=1}^\infty$ with associated probability measures $\{\mathrm{P}_n\}_{n=1}^\infty$ (which are not necessarily consistent). Here, Γ^* is described analogously as E^* in Definition 4. An application of Lemma 3 yields that

$$\Gamma^* \ge \mathrm{P}_n\text{-}\liminf_n \frac{-\log \mathrm{P}_{U_n|V_n}(U_n \mid V_n)}{n}$$
$$\Gamma^* \le \mathrm{P}_n\text{-}\limsup_n \frac{-\log \mathrm{P}_{U_n|V_n}(U_n \mid V_n)}{n}$$

where the first and second limits above equal, respectively, the left- and right-sides of (108) with $\mu_n = \mathrm{P}_n$ and

$$Z_n = \frac{-\log \mathrm{P}_{U_n|V_n}(U_n \mid V_n)}{n}.$$

APPENDIX

A) Proof of Lemma 16: For $1 \le l \le r, 1 \le j \le k$, denote by Φ_{lj} the interactive communication preceding F_{lj}, by $\mathbf{F}_{lj}$ the rv (F_{lj}, Φ_{lj}), and by $\mathbf{i}_{lj}$ a realization of $\mathbf{F}_{lj}$. Without loss of generality, we choose a version of $\tilde{\mathrm{P}}_{Y^k|\mathbf{F}}$ that satisfies

$$\tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}\left(\mathbf{F}_{lj}^{-1}(\mathbf{i}_{lj})^c \mid \mathbf{i}_{lj}\right) = 0, \quad \tilde{\mathrm{P}}_{\mathbf{F}_{lj}} \text{ a.s.}, \tag{A1}$$

for all $1 \le l \le r, 1 \le j \le k$. The following property of interactive communication is pivotal to our proof: for each i_{lj}^-, $\Phi_{lj}^{-1}(i_{lj}^-)$ is a product set, i.e.,

$$\Phi_{lj}^{-1}(i_{lj}^-) = A'_1 \times \cdots \times A'_k, \quad A'_j \in \sigma_j,\ 1 \le j \le k.$$

We prove the claim by induction upon observing that $\tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}$ can be obtained by conditioning $\tilde{\mathrm{P}}_{Y^k|\Phi_{lj}}$ on the rv F_{lj}.

Formally, denote by $\sigma^k(i_{lj}^-) = \sigma_1(i_{lj}^-) \times \cdots \times \sigma_k(i_{lj}^-)$ the σ-field induced by σ^k on $A'_1 \times \cdots \times A'_k$, and by $\sigma\left(F_{lj}(\cdot, i_{lj}^-)\right)$ the smallest sub-σ-field of $\sigma^k(i_{lj}^-)$ with respect to which F_{lj} is measurable (for i_{lj}^- fixed). Using (A1), we choose a version of $\tilde{\mathrm{P}}_{Y^k|\mathbf{F}}$ such that for each $1 \le l \le r$ and $1 \le j \le k$, $\tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}(\cdot \mid \mathbf{i}_{lj})$ is the regular conditional probability on the probability space

$$\left(A'_1 \times \cdots \times A'_k,\ \sigma^k(i_{lj}^-),\ \tilde{\mathrm{P}}_{Y^k|\Phi_{lj}}\left(\cdot \mid i_{lj}^-\right)\right)$$

conditioned on $\sigma\left(F_{lj}(\cdot, i_{lj}^-)\right)$. Specifically

$$\begin{aligned} &\tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}(A \mid \mathbf{i}_{lj}) \\ &\quad = \mathbb{E}_{\tilde{\mathrm{P}}_{Y^k|\Phi_{lj}}(\cdot|i_{lj}^-)}\left[\mathbf{1}_A \mid \sigma\left(F_{lj}(\cdot, i_{lj}^-)\right)\right](i_{lj}), \quad A \in \sigma^k, \end{aligned} \tag{A2}$$

where the underlying σ-field for the conditional expectation is $\sigma^k(i_{lj}^-)$. For this version of $\tilde{\mathrm{P}}_{Y^k|\mathbf{F}}$, we show below that if (96) holds with Φ_{lj} in the role of $\mathbf{F}$, then it holds with $\mathbf{F}_{lj}$ in the role of $\mathbf{F}$. Lemma 16 then follows by induction since (96) holds with $\mathbf{F} = \emptyset$.

It remains to prove the assertion above. To that end, for $B \in \mathcal{F}_{lj}$, denote by $F_{lj}^{-1}\left(B, i_{lj}^-\right)$ the set

$$\left\{y_j \in \mathcal{Y}_j : F_{lj}\left(y_j, i_{lj}^-\right) \in B\right\}.$$

With an abuse of notation, we do not distinguish between the sets $F_{lj}^{-1}\left(B, i_{lj}^-\right)$ and its cylindrical extension

$$\mathcal{Y}_1 \times \cdots \times F_{lj}^{-1}\left(B, i_{lj}^-\right) \times \cdots \times \mathcal{Y}_k.$$

Then, using the notation $\tilde{Q}_{i_{lj}^-}$ and $\tilde{Q}^t_{i_{lj}^-}$, $1 \le t \le k$, for the probability measures $\tilde{\mathrm{P}}_{Y^k|\Phi_{lj}}\left(\cdot \mid i_{lj}^-\right)$ and $\tilde{\mathrm{P}}_{Y_t|\Phi_{lj}}\left(\cdot \mid i_{lj}^-\right)$, $1 \le t \le k$, respectively, our induction hypothesis states

$$\tilde{Q}i_{lj}^-(A_1 \times \cdots . \times A_k) = \prod_{t=1}^{k} \tilde{Q}i_{lj}^-(A_t), \quad A_t \in \sigma_t,\ 1 \le t \le k. \tag{A3}$$

It follows that

$$\begin{aligned}
&\int_{F_{lj}^{-1}(B, i_{lj}^-)} \mathbf{1}_{A_1 \times \cdots \times A_k}\, d\tilde{Q}_{i_{lj}^-} \\
&= \int_{F_{lj}^{-1}(B, i_{lj}^-)} \mathbf{1}_{A_1 \cap A_1' \times \cdots \times A_k \cap A_k'}\, d\tilde{Q}_{i_{lj}^-} \\
&= \left[\prod_{t \neq j} \int \mathbf{1}_{A_t \cap A_t'}\, d\tilde{Q}^t_{i_{lj}^-}\right] \int_{F_{lj}^{-1}(B, i_{lj}^-)} \mathbf{1}_{A_j \cap A_j'}\, d\tilde{Q}^j_{i_{lj}^-},
\end{aligned} \tag{A4}$$

where the first equality uses (A1) and the second uses (A3). Defining

$$P_{lj}^t(A) \triangleq \mathbb{E}_{\tilde{Q}i_{lj}^{-\ t}}\left[\mathbf{1}_A \mid \sigma\left(F_{lj}(\cdot, i_{lj}^-)\right)\right], \qquad A \in \sigma_t(i_{lj}^-),\ 1 \le t \le k,$$

we have from (A4) that

$$\begin{aligned}
&\int_{F_{lj}^{-1}(B, i_{lj}^-)} \mathbf{1}_{A_1 \times \cdots \times A_k}\, d\tilde{Q}_{i_{lj}^-} \\
&= \left[\prod_{t \neq j} \int P_{lj}^t(A_t \cap A_t')\, d\tilde{Q}^t_{i_{lj}^-}\right] \times \\
&\qquad \int_{F_{lj}^{-1}(B, i_{lj}^-)} P_{lj}^j(A_j \cap A_j')\, d\tilde{Q}^j_{i_{lj}^-} \\
&= \int_{F_{lj}^{-1}(B, i_{lj}^-)} \prod_{t=1}^{k} P_{lj}^t(A_t \cap A_t')\, d\tilde{Q}_{i_{lj}^-},
\end{aligned}$$

where the second equality uses (A3). Thus, by (A2)

$$\begin{aligned}
&\tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}\left(A_1 \times \cdots \times A_k \mid \mathbf{i}_{lj}\right) \\
&= \prod_{t=1}^{k} P_{lj}^t(A_t \cap A_t'), \quad \tilde{\mathrm{P}}_{\mathbf{F}_{lj}} \text{ a.s. in } \mathbf{i}_{lj}.
\end{aligned} \tag{A5}$$

Since by (A1) $P_{lj}^t(A_t') = 1$, $1 \le t \le k$, it follows from (A5) that

$$\begin{aligned}
&P_{lj}^t(A_t) \\
&= P_{lj}^t(A_t \cap A_t') \\
&= \tilde{\mathrm{P}}_{Y^k|\mathbf{F}_{lj}}\left(A_1' \times \cdots \times A_{t-1}' \times A_t \times A_{t+1}' \times \cdots \times A_k' \mid \mathbf{i}_{lj}\right) \\
&= \tilde{\mathrm{P}}_{Y_t|\mathbf{F}_{lj}}\left(A_t \mid \mathbf{i}_{lj}\right).
\end{aligned}$$

The previous observation, along with (A5), implies that (96) holds with $\mathbf{F}_{lj}$ in the role $\mathbf{F}$. □

B) Proof of Lemma 17: It suffices to show that the right-side of (98) constitutes a version of $\mathbb{E}_{\tilde{\mathrm{P}}}\left[\mathbf{1}_{A_0} \mid \sigma(\mathbf{F})\right]$, i.e.,

$$\int_{\mathbf{F}^{-1}(B)} \mathbf{1}_{A_0}\, d\tilde{\mathrm{P}} = \int_B \left(\int_{A_0} \frac{d\mathrm{P}_{\mathbf{F}}}{d\tilde{\mathrm{P}}_{\mathbf{F}}}(z) \frac{dQ_z}{d\mathrm{P}}\, d\tilde{\mathrm{P}}\right) \tilde{\mathrm{P}}_{\mathbf{F}}(dz), \tag{A6}$$

for every set B in the range σ-field of $\mathbf{F}$. To show that, we note for every $A \in \sigma^k$ that

$$\begin{aligned}
\int_{\mathbf{F}^{-1}(B)} \mathbf{1}_A\, d\mathrm{P} &= \int_B \mathrm{P}_{Y|\mathbf{F}}\left(A \mid z\right) \mathrm{P}_{\mathbf{F}}(dz) \\
&= \int_B \left(\int_A \frac{dQ_z}{d\mathrm{P}}\, d\mathrm{P}\right) \mathrm{P}_{\mathbf{F}}(dz),
\end{aligned} \tag{A7}$$

where the previous step uses the assumption (86). Using Fubini's and Tonelli's theorems to interchange the order of integrals in (A7), we get

$$\begin{aligned}
\int_{\mathbf{F}^{-1}(B)} \mathbf{1}_A\, d\mathrm{P} &= \int_A \left(\int_B \frac{dQ_z}{d\mathrm{P}} \mathrm{P}_{\mathbf{F}}(dz)\right) d\mathrm{P}, \\
&= \int_A \mathbf{1}_{\mathbf{F}^{-1}(B)}\, d\mathrm{P},
\end{aligned}$$

which further implies

$$\mathbf{1}_{\mathbf{F}^{-1}(B)} = \int_B \frac{dQ_z}{d\mathrm{P}} \mathrm{P}_{\mathbf{F}}(dz), \qquad \mathrm{P} \text{ a.s.}, \tag{A8}$$

since the set $A \in \sigma^k$ was arbitrary. Next, for every B in the range σ-field of $\mathbf{F}$, it follows from (A8) and (97) that

$$\begin{aligned}
\int_{\mathbf{F}^{-1}(B)} \mathbf{1}_{A_0}\, d\tilde{\mathrm{P}} &= \int_{A_0} \mathbf{1}_{\mathbf{F}^{-1}(B)}\, d\tilde{\mathrm{P}} \\
&= \int_{A_0} \frac{1}{d\mathrm{P}/d\tilde{\mathrm{P}}} \mathbf{1}_{\mathbf{F}^{-1}(B)}\, d\mathrm{P} \\
&= \int_{A_0} \frac{1}{d\mathrm{P}/d\tilde{\mathrm{P}}} \int_B \frac{dQ_z}{d\mathrm{P}} \mathrm{P}_{\mathbf{F}}(dz)\, d\mathrm{P} \\
&= \int_{A_0} \int_B \frac{dQ_z}{d\mathrm{P}} \mathrm{P}_{\mathbf{F}}(dz)\, d\tilde{\mathrm{P}}.
\end{aligned} \tag{A9}$$

The claim (A6) follows upon interchanging the order of integrals in (A9). □

ACKNOWLEDGMENT

The authors thank Mokshay Madiman for useful pointers to the work on the AEP for log-concave distributions and related literature [5], [8], which were instrumental in our results for Gaussian rvs in Section VIII. Thanks are also due to an anonymous referee for suggesting the refined definition $E^*(\epsilon, \epsilon')$ discussed in Section IX-B.

REFERENCES

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography-part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[2] E. Arikan, "An inequality on guessing and its application to sequential decoding," *IEEE Trans. Inf. Theory*, vol. 42, no. 1, pp. 99–105, Jan. 1996.

[3] E. Arikan and N. Merhav, "The Shannon cipher system with a guessing wiretapper," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1860–1866, Sep. 1999.

[4] R. B. Ash, *Real Analysis and Probability*. New York, NY, USA: Academic, 1972.

[5] S. Bobkov and M. Madiman, "Concentration of the information in data with log-concave distributions," *Ann. Probab.*, vol. 39, no. 4, pp. 1528–1543, 2011.

[6] C. Chan, "Generating secret in a network," Ph.D. dissertation, Massachusetts Inst. Technol., Cambridge, MA, USA, 2010.

[7] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," in *Proc. 44th Annu. Conf. Inf. Sci. Syst.*, 2010, pp. 1–6.

[8] T. Cover and S. Pombra, "Gaussian feedback capacity," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 37–43, Jan. 1989.

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

[10] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, Jun. 2008.

[11] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Channels*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[12] P. Gács and J. Körner, "Common information is far less than mutual information," *Probl. Control Inf. Theory*, vol. 2, no. 2, pp. 149–162, 1973.

[13] T. S. Han, *Information-Spectrum Methods in Information Theory [English Translation]*, ser. Stochastic Modelling and Applied Probability. New York, NY, USA: Springer-Verlag, 2003, vol. 50.

[14] M. K. Hanawal and R. Sundaresan, "The Shannon cipher system with a guessing wiretapper: General sources," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2503–2516, Apr. 2011.

[15] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May 1993.

[16] G. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1952.

[17] M. Loéve, *Probability Theory*, 2nd ed. New York, NY, USA: Van Nostrand, 1960.

[18] M. Madiman and A. Barron, "Generalized entropy power inequalities and monotonicity properties of information," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2317–2329, Jul. 2007.

[19] M. Madiman, A. Marcus, and P. Tetali, "Entropy and set cardinality inequalities for partition-determined functions," *Random Struct. Algorithms*, vol. 40, pp. 399–424, 2012.

[20] M. Madiman and P. Tetali, "Information inequalities for joint distributions, with interpretations and applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2699–2713, Jun. 2010.

[21] J. L. Massey, "Guessing and entropy," presented at the IEEE Int. Symp. Inf. Theory, Trondheim, Norway, 1994.

[22] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.

[23] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Statist. Prob., (Univ. Calif. Press)*, 1961, vol. 1, pp. 547–561.

[24] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Oct. 1948.

[25] S. Venkatesan and V. Anantharam, "The common randomness capacity of a pair of independent discrete memoryless channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 215–224, Jan. 1998.

Himanshu Tyagi received the Bachelor of Technology degree in electrical engineering and the Master of Technology degree in communication and information technology, both from the Indian Institute of Technology, Delhi, India, in 2007. He is currently a Ph.D. candidate at the University of Maryland, College Park, USA.

Prakash Narayan (F'01) received the Bachelor of Technology degree in Electrical Engineering from the Indian Institute of Technology, Madras in 1976. He received and the M.S. degree in Systems Science and Mathematics in 1978, and the D.Sc. degree in Electrical Engineering, both from Washington University, St. Louis, MO.

He is Professor of Electrical and Computer Engineering at the University of Maryland, College Park, with a joint appointment at the Institute for Systems Research. He has held visiting appointments at ETH, Zurich; the Technion, Haifa; the Renyi Institute of the Hungarian Academy of Sciences, Budapest; the University of Bielefeld; the Institute of Biomedical Engineering (formerly LADSEB), Padova; and the Indian Institute of Science, Bangalore. His research interests are in multiuser information theory, communication theory, communication networks, cryptography, and information theory and statistics.

Dr. Narayan has served as Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY; was Co-Organizer of the IEEE Workshop on Multi-User Information Theory and Systems, VA (1983); Technical Program Chair of the IEEE/IMS Workshop on Information Theory and Statistics, VA (1994); General Co-Chair of the IEEE International Symposium on Information Theory, Washington, D.C. (2001); and Technical Program Co-Chair of the IEEE Information Theory Workshop, Bangalore (2002). He served as a Member of the Board of Governors of the IEEE Information Theory Society from 2007 to 2012.