When Is a Function Securely Computable?

Himanshu Tyagi, Prakash Narayan, *Fellow, IEEE*, and Piyush Gupta, *Fellow, IEEE*

***Abstract*—A subset of a set of terminals that observe correlated signals seek to compute a function of the signals using public communication. It is required that the value of the function be concealed from an eavesdropper with access to the communication. We show that the function is securely computable if and only if its entropy is less than the capacity of a new secrecy generation model, for which a single-letter characterization is provided.**

***Index Terms*—Aided secret key, balanced coloring lemma, function computation, maximum common function, omniscience, secret key capacity, secure computability.**

I. Introduction

In an online auction, $m-1$ bidders acting independently of each other, randomly place one of k bids on a secure server. After a period of independent daily bidding, the server posts a cryptic message on a public website. We shall see that such a message exists from which each bidder can deduce securely the highest daily bids, but for $m > k+1$ no message exists so as to allow any of them to identify securely the daily winners.

In general, suppose that the terminals in $\mathcal{M} = \{1, \ldots, m\}$ observe correlated signals, and that a subset $\mathcal{A} = \{1, \ldots, a\}$ of them are required to compute "securely" a (single-letter) function g of all the signals. To this end, the terminals in $\mathcal{M}$ are allowed to communicate interactively over a public noiseless channel of unlimited capacity, with the communication being observed by all the terminals. The terminals in $\mathcal{A}$ seek to compute g in such a manner as to keep its value information theoretically secret from an eavesdropper that observes the public interterminal communication. Throughout, we assume that the eavesdropper is passive, i.e., unable to tamper with the public communication. A typical application arises in a wireless network of colocated sensors which seek to compute a given function of their correlated measurements using public communication that does not give away the value of the function.

We formulate a new Shannon theoretic multiterminal source model that addresses the elemental question: *When can a function g be computed so that its value is independent of the public communication used in its computation*? We do not tackle the difficult problem of determining the minimum rate of public communication needed for the secure computation of g, which remains open even in the absence of a secrecy constraint [12]. Nor do we fashion efficient protocols for this purpose. Instead, our mere goal in this work is to characterize necessary and sufficient conditions for the *existence* of such protocols.

The study of problems of function computation, with and without secrecy requirements, has a long and varied history in multiple disciplines, to which we can make only a skimpy allusion here. Examples include: algorithms for exact function computation by multiple parties (cf., e.g., [21], [9], [11]); algorithms for asymptotically accurate (in observation length) function computation (cf., e.g., [19], [14]); and problems of oblivious transfer [17], [2]. In contrast, our requirement of secure computation[1] is to protect the value of a given function; an instance is [18] where exact function computation with secrecy was sought.

We establish that the answer to the question posed above is connected innately to a problem of secret key (SK) generation in which all the terminals in $\mathcal{M}$ seek to generate "secret common randomness" of maximum rate, by means of public communication from which an eavesdropper can glean only a negligible amount of information about the SK. The public communication from a terminal can be any function of its own observed signal and of all previous communication. Additionally, side information is provided to the terminals in $\mathcal{A}^c$ in the form of the value of g, and can be used only for recovering the key. Such a key, termed an aided secret key (ASK), constitutes a modification of the original notion of an SK in [15], [1], [6], and [7]. The largest rate of such an ASK is the ASK capacity C. Since a securely computable function g for $\mathcal{A}$ will yield an ASK (for $\mathcal{M}$) of rate equal to the entropy H of g, it is clear that g necessarily must satisfy $H \leq C$. We show that surprisingly, $H < C$ is a sufficient condition for the existence of a protocol for the secure computation of g by $\mathcal{A}$. When all the terminals in $\mathcal{M}$ seek to compute g securely, the corresponding ASK capacity reduces to the standard SK capacity for $\mathcal{M}$ [6], [7]. Furthermore, we show that a function that is securely computed by $\mathcal{A}$ can be augmented by residual secret common randomness to yield an SK for $\mathcal{A}$ of optimum rate.

We also present the capacity for a general ASK model involving *arbitrary* side information at the secrecy-seeking set of terminals; such side information is not available for communication and can be used for key recovery alone. Its capacity is characterized in terms of the classic concept of "maximum common function" [8]. Although this result is not needed in full dose for characterizing secure computability, it remains of independent interest.

[1]Unlike in [21] and allied literature, no key is available *apriori* for secure computation but may be devised as a part of the computation procedure.

Manuscript received July 17, 2010; revised April 25, 2011; accepted May 27, 2011. Date of current version October 07, 2011. H. Tyagi and P. Narayan were supported by the U.S. National Science Foundation under Grants CCF0635271 and CCF0830697. P. Gupta was supported by NSF Grant CNS-519535. The material in this paper was presented in part at the 2010 IEEE International Symposium on Information Theory and in part at the 2011 IEEE International Symposium on Information Theory.

H. Tyagi and P. Narayan 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).

P. Gupta is with Bell Labs, Alcatel-Lucent, Murray Hill, NJ 07974 USA (e-mail: pgupta@research.bell-labs.com).

Communicated by S. N. Diggavi, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2011.2165807

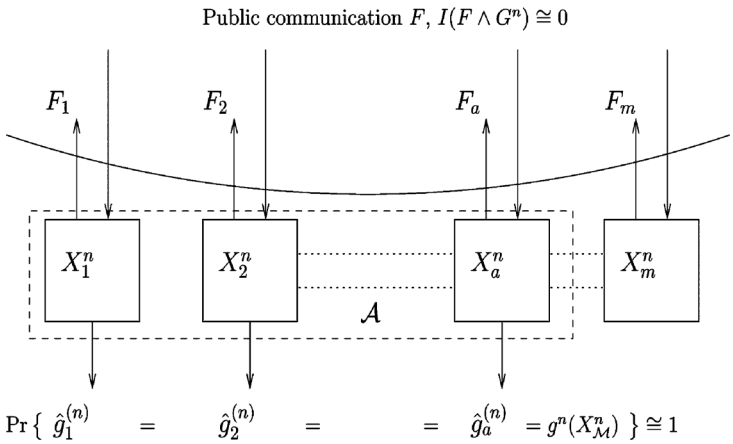

Fig. 1. Secure computation of g.

Our results in Section III are organized in three parts: capacity of the ASK model; characterization of the secure computability of g; and a decomposition result for the total entropy of the model. Proofs are provided in Section IV and concluding remarks in Section V.

II. Preliminaries

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). For any nonempty set $A \subseteq \mathcal{M} = \{1, \ldots, m\}$, we denote $X_A = (X_i,\ i \in \mathcal{A})$. Similarly, for real numbers $R_1, \ldots, R_m$ and $A \subseteq \mathcal{M}$, we denote $R_A = (R_i,\ i \in A)$. Let $\mathcal{A}^c$ be the set $\mathcal{M} \backslash A$. We denote n i.i.d. repetitions of $X_{\mathcal{M}} = (X_1, \ldots, X_m)$ with values in $\mathcal{X}_{\mathcal{M}} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_m$ by $X_{\mathcal{M}}^n = (X_1^n, \ldots, X_m^n)$ with values in $\mathcal{X}_{\mathcal{M}}^n = \mathcal{X}_1^n \times \ldots \times \mathcal{X}_m^n$. Following [6], given $\epsilon > 0$, for rvs U, V, we say that U is *ϵ-recoverable* from V if $\Pr(U \neq f(V)) \leq \epsilon$ for some function $f(V)$ of V. All logarithms and exponentials are with respect to the base 2.

We consider a multiterminal source model for secure computation with public communication; this basic model was introduced in [6] in the context of SK generation with public transaction. Terminals $1, \ldots, m$ observe, respectively, the sequences $X_1^n, \ldots, X_m^n$, of length n. Let $g : \mathcal{X}_{\mathcal{M}} \to \mathcal{Y}$ be a given mapping, where $\mathcal{Y}$ is a finite alphabet. For $n \geq 1$, the mapping $g^n : \mathcal{X}_{\mathcal{M}}^n \to \mathcal{Y}^n$ is defined by

$$g^n(x_{\mathcal{M}}^n) = (g(x_{11}, \ldots, x_{m1}), \ldots, g(x_{1n}, \ldots, x_{mn})),$$
$$x_{\mathcal{M}}^n = (x_1^n, \ldots, x_m^n) \in \mathcal{X}_{\mathcal{M}}^n.$$

For convenience, we shall denote the rv $g^n\left(X_{\mathcal{M}}^n\right)$ by $G^n, n \geq 1$, and, in particular, $G^1 = g\left(X_{\mathcal{M}}\right)$ simply by G. The terminals in a given set $\mathcal{A} \subseteq \mathcal{M}$ wish to "compute securely" the function $g^n(x_{\mathcal{M}}^n)$ for $x_{\mathcal{M}}^n$ in $\mathcal{X}_{\mathcal{M}}^n$. To this end, the terminals are allowed to communicate over a noiseless public channel, possibly interactively in several rounds. Randomization at the terminals is permitted; we assume that terminal i generates a rv $U_i,\ i \in \mathcal{M}$, such that $U_1, \ldots, U_m$ and $X_{\mathcal{M}}^n$ are mutually independent. While the cardinalities of range spaces of $U_i, i \in \mathcal{M}$, are unrestricted, we assume that $H\left(U_{\mathcal{M}}\right) < \infty$.

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; 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 (U_i, X_i^n) and of previous communication described in terms of $\{f_{kl} : k < j,\ l \in \mathcal{M}$ or $k = j,\ l < i\}$. The corresponding rvs representing the communication will be depicted collectively as

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

where $\mathbf{F} = \mathbf{F}^{(n)}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$. A special form of such communication will be termed *noninteractive communication* if $\mathbf{F} = (F_1, \ldots, F_m)$, where $F_i = f_i\left(U_i, X_i^n\right), i \in \mathcal{M}$.

Definition 2: For $\epsilon_n > 0, n \geq 1$, we say that g is *ϵ_n-securely computable* (ϵ_n- SC) by (the terminals in) a given set $\mathcal{A} \subseteq \mathcal{M}$ with $|\mathcal{A}| \geq 1$ from observations of length n, randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F} = \mathbf{F}^{(n)}$, if
(i) g^n is ϵ_n-recoverable from $(U_i, X_i^n, \mathbf{F})$ for every $i \in \mathcal{A}$, i.e., there exists $\hat{g}_i^{(n)}$ satisfying

$$\Pr\left(\hat{g}_i^{(n)}\left(U_i, X_i^n, \mathbf{F}\right) \neq G^n\right) \leq \epsilon_n, \quad i \in \mathcal{A} \tag{1}$$

and
(ii) g^n satisfies the "strong" secrecy condition[2]

$$I(G^n \wedge \mathbf{F}) \leq \epsilon_n. \tag{2}$$

By definition, an ϵ_n-SC function g is recoverable (as g^n) at the terminals in $\mathcal{A}$ and is effectively concealed from an eavesdropper with access to the public communication $\mathbf{F}$.

Definition 3: We say that g is *securely computable* by $\mathcal{A}$ if g is ϵ_n-SC by $\mathcal{A}$ from observations of length n, suitable randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F}$, such that $\lim_n \epsilon_n = 0$.

Fig. 1 shows our setup for secure computing.

[2]The notion of strong secrecy for SK generation was introduced in [16], and developed further in [4], [5].

III. When Is G Securely Computable?

We consider first the case when all the terminals in $\mathcal{M}$ wish to compute securely the function g, i.e., $\mathcal{A} = \mathcal{M}$. Our result for this case will be seen to be linked inherently to the standard concept of SK capacity for a multiterminal source model [6], [7], and serves to motivate our approach to the general case when $\mathcal{A} \subseteq \mathcal{M}$.

Definition 4: [6], [7] For $\epsilon_n > 0, n \geq 1$, a function K of $X_{\mathcal{M}}^n$ is an ϵ_n-*secret key* (ϵ_n-SK) for (the terminals in) a given set[3] $\mathcal{A}' \subseteq \mathcal{M}$ with $|\mathcal{A}'| \geq 2$, achievable from observations of length n, randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F} = \mathbf{F}^{(n)}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$ as above if
(i) K is ϵ_n-recoverable from $(U_i, X_i^n, \mathbf{F})$ for every $i \in \mathcal{A}'$;
(ii) K satisfies the "strong" secrecy condition

$$\log |\mathcal{K}| - H(K \mid \mathbf{F}) = \log |\mathcal{K}| - H(K) + I(K \wedge \mathbf{F}) \leq \epsilon_n \tag{3}$$

where $\mathcal{K} = \mathcal{K}^{(n)}$ denotes the set of possible values of K. The SK capacity $C(\mathcal{A}')$ for $\mathcal{A}'$ is the largest rate $\lim\limits_n (1/n) \log H(K)$ of ϵ_n-SKs for $\mathcal{A}'$ as above,[4] such that $\lim\limits_n \epsilon_n = 0$.

Remark: The secrecy condition (3) is tantamount jointly to a nearly uniform distribution for K (i.e., $\log |\mathcal{K}| - H(K)$ is small) and to the near independence of K and $\mathbf{F}$ (i.e., $I(K \wedge \mathbf{F})$ is small).

A single-letter characterization of the SK capacity $C(\mathcal{A}')$ is provided in [6], [7].

Theorem 1: [6], [7] The SK capacity $C(\mathcal{A}')$ equals

$$C(\mathcal{A}') = H(X_{\mathcal{M}}) - R_{CO}(\mathcal{A}'), \tag{4}$$

where

$$R_{CO}(\mathcal{A}') = \min_{R_{\mathcal{M}} \in \mathcal{R}(\mathcal{A}')} \sum_{i=1}^{m} R_i \tag{5}$$

with

$$\mathcal{R}(\mathcal{A}') = \left\{ R_{\mathcal{M}} : \sum_{i \in B} R_i \geq H(X_B \mid X_{B^c}), \right. \\ \left. B \subsetneq \mathcal{M}, \mathcal{A}' \nsubseteq B \right\}. \tag{6}$$

Furthermore, the SK capacity can be achieved with noninteractive communication and without recourse to randomization at the terminals in $\mathcal{M}$.

Remarks: (i) For the trivial case $|\mathcal{A}'| = 1$, say with $\mathcal{A}' = \{1\}$, we have that $C(\{1\}) = H(X_1)$. Clearly, $K = X_1^n$ attains $C(\{1\})$. On the other hand, if $K = K(X_{\mathcal{M}}^n)$ is an SK for terminal 1, it is also an SK for a relaxed model where terminal 1 remains the same while terminals $2, \ldots, m$ coalesce and have additional access to X_1^n. The SK capacity for the latter model with two terminals, which is no smaller than $C(\{1\})$, equals $I(X_1 \wedge X_{\mathcal{M}}) = H(X_1)$ [15], [1]. Hence, $C(\{1\}) = H(X_1)$.
(ii) The SK capacity $C(\mathcal{A}')$ is not increased if the secrecy condition (3) is replaced by the following weaker requirement [15], [6]:

$$\frac{1}{n} I(K \wedge \mathbf{F}) \leq \epsilon_n. \tag{7}$$

We recall from [6] that $R_{CO}(\mathcal{A}')$ has the operational significance of being the smallest rate of "communication for omniscience" for $\mathcal{A}'$, namely the smallest rate $\lim\limits_n (1/n) \log \|\mathbf{F}^{(n)}\|$ of suitable communication for the terminals in $\mathcal{M}$ whereby $X_{\mathcal{M}}^n$ is ϵ_n-recoverable from $(U_i, X_i^n, \mathbf{F}^n)$ at each terminal $i \in \mathcal{A}'$, with $\lim\limits_n \epsilon_n = 0$; here $\|\mathbf{F}^{(n)}\|$ denotes the cardinality of the set of values of $\mathbf{F}^{(n)}$. Thus, $R_{CO}(\mathcal{A}')$ is the smallest rate of communication among the terminals in $\mathcal{M}$ that enables every terminal in $\mathcal{A}'$ to reconstruct with high probability all the sequences observed by all the other terminals in $\mathcal{M}$, with the cooperation of the terminals in $\mathcal{M}/\mathcal{A}'$. The resulting omniscience for $\mathcal{A}'$ corresponds to total "common randomness" of rate $H(X_{\mathcal{M}})$. The notion of omniscience was introduced in [6], where it played a central role in SK generation for the multiterminal source model; it will play a material role in the secure computation of g as well.

A comparison of the conditions in (2) and (7) that must be met by a securely computable g and an SK K, respectively, shows for a given g to be securely computable, it is necessary that

$$H(G) \leq C(\mathcal{M}). \tag{8}$$

Remarkably, it transpires that $H(G) < C(\mathcal{M})$ is a sufficient condition for g to be securely computable, and constitutes our first result.

Theorem 2: A function g is securely computable by $\mathcal{M}$ if

$$H(G) < C(\mathcal{M}). \tag{9}$$

Conversely, if g is securely computable by $\mathcal{M}$, then $H(G) \leq C(\mathcal{M})$.

Theorem 2 is, in fact, a special case of our main result in Theorem 5 below.

Example 1: Let $m = 2$, and let X_1 and X_2 be $\{0,1\}$-valued rvs with

$$P_{X_1}(1) = p = 1 - P_{X_1}(0), \quad 0 < p < 1,$$
$$P_{X_2|X_1}(1 \mid 0) = P_{X_2|X_1}(0 \mid 1) = \delta, \quad 0 < \delta < \frac{1}{2}.$$

Let $g(x_1, x_2) = x_1 + x_2 \bmod 2$.

From [15], [1] (and also Theorem 1), $C(\{1,2\}) = h(p * \delta) - h(\delta)$, where $p * \delta = (1-p)\delta + p(1-\delta)$. Since $H(G) = h(\delta)$, by Theorem 2 g is securely computable if

$$2h(\delta) < h(p * \delta). \tag{10}$$

We give a simple scheme for the secure computation of g when $p = 1/2$, that relies on Wyner's well-known method

[3] For reasons of notation that will be apparent later, we distinguish between the secrecy seeking set $\mathcal{A}' \subseteq \mathcal{M}$ and the set $\mathcal{A} \subseteq \mathcal{M}$ pursuing secure computation.

[4] In [6], [7], a secret key was defined, in general, as $K = K(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$ and SK capacity was shown to be achieved by a function of $X_{\mathcal{M}}^n$. Also, in view of (3), SK rate can be defined as $\lim\limits_n \frac{1}{n} \log |\mathcal{K}^{(n)}|$.

for Slepian-Wolf data compression [20] and a derived SK generation scheme in [23], [24], and [22]. When $p = 1/2$, we can write

$$X_1^n = X_2^n + G^n \mod 2 \tag{11}$$

with G^n being independent separately of X_2^n and X_1^n. We observe as in [20] that there exists a binary linear code, of rate $\cong 1 - h(\delta)$, with parity check matrix $\mathbf{P}$ such that X_1^n, and so G^n, is ϵ_n-recoverable from (F_1, X_2^n) at terminal 2, where the Slepian-Wolf codeword $F_1 = \mathbf{P}X_1^n$ constitutes public communication from terminal 1, and where ϵ_n decays to 0 exponentially rapidly in n. Let $\widehat{G^n}$ be the estimate of G^n thereby formed at terminal 2. (We can take $\widehat{G^n}$ to have been compressed losslessly to rate $H(G)$.) Further, let $K = K(X_1^n)$ be the location of X_1^n in the coset of the standard array corresponding to $\mathbf{P}$. By the previous observation, K too is ϵ_n-recoverable from (F_1, X_2^n) at terminal 2. From [23], [24], [22], K constitutes a "perfect" SK for terminals 1 and 2, of rate $\cong I(X_1 \wedge X_2) = 1 - h(\delta)$, and satisfying

$$I(K \wedge F_1) = 0. \tag{12}$$

Also, observe from (11) that $K = K(X_1^n) = K(X_2^n + G^n)$ and $F_1 = F_1(X_1^n) = F_1(X_2^n + G^n)$. Since G^n is independent of X_2^n, it follows that conditioned on each fixed value $G^n = g^n$, the (common) argument of K and F_1, namely $X_2^n + G^n$, has a conditional pmf that equals the pmf of $X_2^n + g^n$ which, in turn, coincides with the pmf of $X_1^n + g^n$, i.e., a permutation of the pmf of X_1^n. Hence by (12),

$$I(K \wedge F_1, G^n) = I(K \wedge F_1 \mid G^n) = 0 \tag{13}$$

since $I(K \wedge G^n) \le I(X_1^n \wedge G^n) = 0$.

Then terminal 2 communicates $\widehat{G^n}$ in encrypted form as

$$F_2 = \widehat{G^n} + K \mod 2$$

(all represented in bits), with encryption feasible since

$$H(G) = h(\delta) < 1 - h(\delta) \cong \frac{1}{n} H(K),$$

by the sufficient condition (10). Terminal 1 then decrypts F_2 using K to recover $\widehat{G^n}$. The computation of g^n is secure since

$$I(G^n \wedge F_1, F_2) = I(G^n \wedge F_1) + I(G^n \wedge F_2 \mid F_1)$$

is small; specifically, the first term equals 0 since $I(G^n \wedge F_1) \le I(G^n \wedge X_1^n) = 0$, while the second term is bounded according to

$$\begin{aligned} I(G^n \wedge F_2 \mid F_1) &= H(\widehat{G^n} + K \mid F_1) - H(\widehat{G^n} + K \mid F_1, G^n) \\ &\le H(K) - H(G^n + K \mid F_1, G^n) + \delta_n, \\ &\qquad \text{with } \delta_n \to 0 \\ &= I(K \wedge F_1, G^n) + \delta_n = \delta_n \end{aligned}$$

where the intermediate step uses Fano's inequality and the exponential decay of ϵ_n to 0, and the last equality is by (13). □

Example 2: Consider the setup of Example 1 for the case $p = 1/2$, but now with terminal 1 alone seeking to compute g. Since G^n is independent of X_2^n, secure computation of g at terminal 1 is possible with terminal 2 simply communicating X_2^n, even when X_1 and X_2 are independent. Note that

$$H(G) = h(\delta) \le C(\{1\}) = H(X_1) = 1$$

for $0 \le \delta \le 1/2$. □

We now turn to the general model for the secure computability of g by a given set $\mathcal{A} \subseteq \mathcal{M}$. Again in the manner of (8), it is clear that a necessary condition is

$$H(G) \le C(\mathcal{A}).$$

In contrast, when $\mathcal{A} \subsetneq \mathcal{M}$, the condition $H(G) < C(\mathcal{A})$ is *not* sufficient for g to be securely computable by $\mathcal{A}$ as seen by the following simple example.

Example 3: Let $m = 3$, $A = \{1, 2\}$ and consider rvs X_1, X_2, X_3 with $X_1 = X_2$, where X_1 is independent of X_3 and $H(X_3) < H(X_1)$. Let g be defined by $g(x_1, x_2, x_3) = x_3$, $x_i \in \mathcal{X}_i$, $1 \le i \le 3$. Clearly, $C(\{1, 2\}) = H(X_1)$. Therefore, $H(G) = H(X_3) < C(\{1, 2\})$. However, for g to be computed by the terminals 1 and 2, its value must be conveyed to them necessarily by public communication from terminal 3. Thus, g is not securely computable. □

We observe in Example 2 that if the value of G^n is given to terminal 2 after it has communicated X_2^n to terminal 1, then both terminals attain omniscience, with terminal 1 doing so from communication that is independent of G^n. Terminal 1 then computes G^n from its omniscience. Interestingly, the secure computability of g can be examined in terms of a new SK generation problem that contains these features and is formulated next.

A. Secret Key Aided by Side Information

We consider an extension of the SK generation problem in Definition 4, which involves additional side information $Z_{\mathcal{A}'}^n$ that is correlated with $X_{\mathcal{M}}^n$ and is provided to the terminals in $\mathcal{A}'$ for use in *only the recovery stage* of SK generation; however, the public communication $\mathbf{F}$ remains as in Definition 1. Formally, the extension is described in terms of generic rvs $(X_1, \ldots, X_m, \{Z_i, i \in \mathcal{A}'\})$, where the rvs Z_i too take values in finite sets $\mathcal{Z}_i$, $i \in \mathcal{A}'$. The full force of this extension will not be needed to characterize the secure computability of g; an appropriate particularization will suffice. Nevertheless, this concept is of independent interest.

Definition 5: A function K of $(X_{\mathcal{M}}^n, Z_{\mathcal{A}'}^n)$ is an ϵ_n- secret key aided by side information $Z_{\mathcal{A}'}^n$ (ϵ_n-ASK) for the terminals $\mathcal{A}' \subseteq \mathcal{M}$, $|\mathcal{A}'| \ge 2$, achievable from observations of length n, randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F} = \mathbf{F}(U_{\mathcal{M}}, X_{\mathcal{M}}^n)$ if it satisfies the conditions in Definition 4 with $(U_i, X_i^n, Z_i^n, \mathbf{F})$ in the role of $(U_i, X_i^n, \mathbf{F})$ in condition (i). The corresponding ASK capacity $C(\mathcal{A}', Z_{\mathcal{A}'})$ is defined analogously as in Definition 4.

In contrast with the omniscience rate of $H(X_{\mathcal{M}})$ that appears in the passage following Theorem 1, now an underlying analogous notion of omniscience will involve total common randomness of rate exceeding $H(X_{\mathcal{M}})$. Specifically, the enhanced

common randomness rate will equal the entropy of the "maximum common function" (mcf) of the rvs $(X_{\mathcal{M}}, Z_i)_{i\in\mathcal{A}}$, introduced for a pair of rvs in [8] (see also [3, Problem 16.27]).

Definition 6: [8] For two rvs Q, R with values in finite sets $\mathcal{Q}, \mathcal{R}$, the equivalence relation $q \sim q'$ in $\mathcal{Q}$ holds if there exist $N \geq 1$ and sequences $(q_0, q_1, \ldots, q_N)$ in $\mathcal{Q}$ with $q_0 = q$, $q_N = q'$ and $(r_1, \ldots, r_N)$ in $\mathcal{R}$ satisfying $\Pr(Q = q_{l-1}, R = r_l) > 0$ and $\Pr(Q = q_l, R = r_l) > 0$, $l = 1, \ldots, N$. Denote the corresponding equivalence classes in $\mathcal{Q}$ by $\mathcal{Q}_1, \ldots, \mathcal{Q}_k$. Similarly, let $\mathcal{R}_1, \ldots, \mathcal{R}_{k'}$ denote the equivalence classes in $\mathcal{R}$. As argued in [8], $k = k'$ and for $1 \leq i, j \leq k$,

$$\begin{aligned}\Pr(Q \in \mathcal{Q}_i \mid R \in \mathcal{R}_j) &= \Pr(R \in \mathcal{R}_j \mid Q \in \mathcal{Q}_i) \\ &= \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}\end{aligned}$$

The mcf of the rvs Q, R is a rv $\mathtt{mcf}(Q, R)$ with values in $\{1, \ldots, k\}$, defined by

$$\mathtt{mcf}(Q, R) = i \quad \text{iff} \quad Q \in \mathcal{Q}_i, R \in \mathcal{R}_i, \quad i = 1, \ldots, k.$$

For rvs $Q_1, \ldots, Q_m$ taking values in finite alphabets, we define the $\mathtt{mcf}(Q_1, \ldots, Q_m)$ recursively by

$$\mathtt{mcf}(Q_1, \ldots, Q_m) = \mathtt{mcf}(\mathtt{mcf}(Q_1, \ldots, Q_{m-1}), Q_m) \tag{14}$$

with $\mathtt{mcf}(Q_1, Q_2)$ as above.

Definition 7: With Q^n denoting n i.i.d. repetitions of the rv Q, we define

$$\mathtt{mcf}^n(Q_1, \ldots, Q_m) = \{\mathtt{mcf}(Q_{1t}, \ldots, Q_{mt})\}_{t=1}^n. \tag{15}$$

Note that $\mathtt{mcf}^n(Q_1, \ldots, Q_m)$ is a function of *each* individual $Q_i^n, i = 1, \ldots, m$.

Remark: As justification for the definition in (14), consider a rv ξ that satisfies

$$H(\xi \mid Q_i) = 0, \quad i = 1, \ldots, m \tag{16}$$

and suppose for any other rv ξ' satisfying (16) that $H(\xi) \geq H(\xi')$. Then Lemma 3 below shows that ξ must satisfy $H(\xi) = H(\mathtt{mcf}(Q_1, \ldots, Q_m))$.

The following result for the mcf of $m \geq 2$ rvs is a simple extension of the classic result for $m = 2$ [8, Theorem 1].

Lemma 3: Given $0 < \epsilon < 1$, if $\xi^{(n)}$ is ϵ-recoverable from Q_i^n for each $i = 1, \ldots, m$, then

$$\limsup_n \frac{1}{n} H\left(\xi^{(n)}\right) \leq H(\mathtt{mcf}(Q_1, \ldots, Q_m)). \tag{17}$$

Proof: The proof involves a recursive application of [8, Lemma, Sect. 4] to $\mathtt{mcf}(Q_1, \ldots, Q_m)$ in (14), and is provided in Appendix A.

We are now in a position to characterize ASK capacity. In a manner analogous to Theorem 1, this is done in terms of $H(\mathtt{mcf}(X_{\mathcal{M}}, Z_i)_{i\in\mathcal{A}'})$ and the smallest rate of communication $R_{CO}(\mathcal{A}', Z_{\mathcal{A}'})$ for each terminal in $\mathcal{A}'$ to attain omniscience that corresponds to n i.i.d. repetitions of $\mathtt{mcf}((X_{\mathcal{M}}, Z_i)_{i\in\mathcal{A}'})$.

Theorem 4: The ASK capacity $C(\mathcal{A}'; Z_{\mathcal{A}'})$ equals

$$C(\mathcal{A}'; Z_{\mathcal{A}'}) = H(\mathtt{mcf}((X_{\mathcal{M}}, Z_i)_{i\in\mathcal{A}'})) - R_{CO}(\mathcal{A}'; Z_{\mathcal{A}'})$$

where

$$R_{CO}(\mathcal{A}'; Z_{\mathcal{A}'}) = \min_{R_{\mathcal{M}} \in \mathcal{R}(\mathcal{A}'; Z_{\mathcal{A}'})} \sum_{i\in\mathcal{M}} R_i$$

with

$$\mathcal{R}(\mathcal{A}'; Z_{\mathcal{A}'}) = \left\{ R_{\mathcal{M}} : \sum_{i\in B} R_i \geq \max_{j \in B^c \cap \mathcal{A}'} H(X_B \mid X_{B^c}, Z_j), \right. \\ \left. B \subsetneq \mathcal{M}, \mathcal{A}' \nsubseteq B \right\}. \tag{18}$$

The proof of Theorem 4 is along the same lines as that of Theorem 1 [6] and is provided in Appendix B.

The remark following Theorem 1 also applies to the ASK capacity $C(\mathcal{A}'; Z_{\mathcal{A}'})$, as will be seen from the proof of Theorem 4.

B. Characterization of Secure Computability

If g is securely computable by the terminals in $\mathcal{A}$, then G^n constitutes an ASK for $\mathcal{M}$ under the constraint (7), of rate $H(G)$, with side information in the form of G^n provided only to the terminals in $\mathcal{A}^c$ in the recovery stage of SK generation. Thus, a necessary condition for g to be securely computable by $\mathcal{A}$, in the manner of (8), is

$$H(G) \leq C(\mathcal{M}; Z_{\mathcal{M}}) \tag{19}$$

where $Z_{\mathcal{M}} = Z_{\mathcal{M}}(\mathcal{A}) = \{Z_i\}_{i\in\mathcal{M}}$ with

$$Z_i = \begin{cases} 0, & i \in \mathcal{A} \\ G, & i \in \mathcal{A}^c. \end{cases} \tag{20}$$

By particularizing Theorem 4 to the choice of $Z_{\mathcal{M}}$ as above, the right-hand side (RHS) of (19) reduces to

$$C(\mathcal{M}; Z_{\mathcal{M}}) = H(X_{\mathcal{M}}) - R_{CO}(\mathcal{M}; Z_{\mathcal{M}}) \tag{21}$$

where

$$R_{CO}(\mathcal{M}; Z_{\mathcal{M}}) = \min_{R_{\mathcal{M}} \in \mathcal{R}(\mathcal{M}; Z_{\mathcal{M}})} \sum_{i\in\mathcal{M}} R_i$$

with

$$\mathcal{R}(\mathcal{M}; Z_{\mathcal{M}}) = \\ \left\{ R_{\mathcal{M}} : \sum_{i\in B} R_i \geq \begin{cases} H(X_B \mid X_{B^c}), & B \subsetneq \mathcal{M}, \mathcal{A} \nsubseteq B \\ H(X_B \mid X_{B^c}, G), & B \subsetneq \mathcal{M}, \mathcal{A} \subseteq B \end{cases} \right\}. \tag{22}$$

Our main result says that the necessary condition (19) is tight. Consider a protocol that enables the terminals in $\mathcal{M}$ to attain omniscience using communication that is independent of G^n, when G^n is provided only as "decoder side information" to the terminals in $\mathcal{A}^c$ but cannot be used for communication. Our

proof shows that (23) below is sufficient for such a protocol to exist. Clearly, this protocol also serves for the secure computation of g by the terminals in $\mathcal{A}$ upon disregarding the decoding tasks in $\mathcal{A}^c$ (so that the protocol does not depend on a knowledge of G^n).

Theorem 5: A function g is securely computable by $\mathcal{A} \subseteq \mathcal{M}$ if

$$H(G) < C(\mathcal{M}; Z_{\mathcal{M}}). \tag{23}$$

Furthermore, under the condition above, g is securely computable with noninteractive communication and without recourse to randomization at the terminals in $\mathcal{M}$.

Conversely, if g is securely computable by $\mathcal{A} \subseteq \mathcal{M}$, then $H(G) \leq C(\mathcal{M}; Z_{\mathcal{M}})$.

Remarks: (i) As in the proof of achievability of SK capacity in [6], our proof of the sufficiency of (23) for the secure computability of g holds with ϵ_n in (1), (2) decaying to zero exponentially rapidly in n.
(ii) It is easy to see that $C(\mathcal{M}) \leq C(\mathcal{M}; Z_{\mathcal{M}}) \leq C(\mathcal{A})$, where $Z_{\mathcal{M}}$ is as in (20). In particular, the second inequality holds by noting that an SK for $\mathcal{M}$ is also an SK for $\mathcal{A}$, and that the side information for recovery $Z_{\mathcal{M}}$ in (20) is not provided to the terminals in $\mathcal{A}$.
(iii) Observe in Example 3 that $C(\mathcal{M}; Z_{\mathcal{M}}) = C(\mathcal{M}) = 0$ and so, by Theorem 5, g is not securely computable as noted earlier.

Example 4: For the auction example in Section I, $\mathcal{A} = \{1, \ldots, m-1\}$ and $X_1, \ldots, X_{m-1}$ are i.i.d. rvs distributed uniformly on $\{1, \ldots, k\}$, while $X_m = (X_1, \ldots, X_{m-1})$. Let $g_1(x_1, \ldots, x_m) = \max\limits_{1 \leq i \leq m-1} x_i$ and $g_2(x_1, \ldots, x_m) = \arg \max\limits_{1 \leq i \leq m-1} x_i$. Then, straightforward computation yields that

$$H(G_1) < \log k$$

and for both g_1, g_2 that

$$C(\mathcal{M}; Z_{\mathcal{M}}) = C(\mathcal{M})$$

where, by Theorem 1

$$\begin{aligned} C(\mathcal{M}) &= H(X_{\mathcal{M}}) - R_{CO}(\mathcal{M}) \\ &= (m-1)\log k - (m-2)\log k = \log k. \end{aligned} \tag{24}$$

Hence, by Theorem 5, g_1 is securely computable. Since

$$H(G_2) = \log(m-1)$$

g_2 is securely computable if $k > m-1$. However, for $k < m-1$, g_2 is not securely computable by *any* terminal $i \in \{1, \ldots, m-1\}$. This, too, is implied by Theorem 5 upon noting that for each $i \in \{1, \ldots, m-1\}$ and a restricted choice $\mathcal{A} = \{i\}$ and $Z_{\mathcal{M}}$ as in (20)

$$C(\mathcal{M}; Z_{\mathcal{M}}) = H(X_i) = \log k < \log(m-1) = H(G_2)$$

where the first equality is a consequence of remark (ii) following Theorem 5, (24) and remark (i) following Theorem 1. □

C. A Decomposition Result

The sufficiency condition (23) prompts the following two natural questions: Does the difference $C(\mathcal{M}; Z_{\mathcal{M}}) - H(G)$ possess an operational significance? If g is securely computable by the terminals in $\mathcal{A}$, clearly G^n forms an SK for $\mathcal{A}$. Can G^n be augmented suitably to form an SK for $\mathcal{A}$ of maximum achievable rate?

The answers to both these questions are in the affirmative. In particular, our approach to the second question involves a characterization of the minimum rate of communication for omniscience for $\mathcal{A}$, under the additional requirement that this communication be independent of G^n. Specifically, we show below that for a securely computable function g, this minimum rate remains $R_{CO}(\mathcal{A})$ [see (5) and (6)].

Addressing the first question, we introduce a rv $K_g = K_g^{(n)}$ such that $K = (K_g, G^n)$ constitutes an ϵ_n-ASK for $\mathcal{M}$ with side information $Z_{\mathcal{M}}$ as in (20) and satisfying the additional requirement

$$I(K_g \wedge G^n) \leq \epsilon_n. \tag{25}$$

Let the largest rate $\lim_n (1/n) H(K_g)$ of such an ASK be $C^g(\mathcal{M}; Z_{\mathcal{M}})$. Observe that since K is required to be nearly independent of $\mathbf{F}$, where $\mathbf{F}$ is the public communication involved in its formation, it follows by (25) that K_g is nearly independent of $(G^n, \mathbf{F})$.

Turning to the second question, in the same vein let K_g' be a rv such that $K' = \left(K_g', G^n\right)$ constitutes an ϵ_n-SK for $\mathcal{A} \subseteq \mathcal{M}$ and satisfying (25). Let $C^g(\mathcal{A})$ denote the largest rate of K_g'. As noted above, K_g' will be nearly independent of $(G^n, \mathbf{F}')$, where $\mathbf{F}'$ is the public communication involved in the formation of K'.

Proposition 6: If g satisfies (23), for $\mathcal{A} \subseteq \mathcal{M}$ it holds that

$$\begin{aligned} &(i) \quad C^g(\mathcal{M}; Z_{\mathcal{M}}(\mathcal{A})) = C(\mathcal{M}; Z_{\mathcal{M}}(\mathcal{A})) - H(G), \\ &(ii) \quad C^g(\mathcal{A}) = C(\mathcal{A}) - H(G). \end{aligned}$$

Remarks: (i) For the case $\mathcal{A} = \mathcal{M}$, both (i) and (ii) above reduce to $C^g(\mathcal{M}) = C(\mathcal{M}) - H(G)$.
(ii) Theorem 1 and Proposition 6 (ii) lead to the observation

$$H(X_{\mathcal{M}}) = R_{CO}(\mathcal{A}) + H(G) + C^g(\mathcal{A})$$

which admits the following heuristic interpretation. The "total randomness" $X_{\mathcal{M}}^n$ that corresponds to omniscience decomposes into three "nearly mutually independent" components: a minimum-sized communication for omniscience for $\mathcal{A}$ and the independent parts of an optimum-rate SK for $\mathcal{A}$ composed of G^n and K_g'.

IV. Proofs of Theorem 5 and Proposition 6

A. Proof of Theorem 5

The necessity of (19) follows by the comments preceding Theorem 5.

The sufficiency of (23) will be established by showing the existence of *noninteractive* public communication comprising source codes that enable omniscience corresponding to $X_{\mathcal{M}}^n$ at

the terminals in $\mathcal{A}$, and thereby the computation of g. Furthermore, the corresponding codewords are selected so as to be simultaneously independent of G^n, thus assuring security.

First, from (23) and (21), there exists $\delta > 0$ such that $R_{CO}(\mathcal{M}; Z_{\mathcal{M}}) + \delta < H(X_{\mathcal{M}}|G)$, using $G = g(X_{\mathcal{M}})$. For each i and $R_i \geq 0$, consider a (map-valued) rv J_i that is uniformly distributed on the family $\mathcal{J}_i$ of all mappings $\mathcal{X}_i^n \to \{1, \ldots, \lceil \exp(nR_i) \rceil\}, i \in \mathcal{M}$. The rvs $J_1, \ldots, J_m, X_{\mathcal{M}}^n$ are taken to be mutually independent.

Fix ϵ, ϵ', with $\epsilon' > m\epsilon$ and $\epsilon + \epsilon' < 1$. It follows from the proof of the general source network coding theorem [3, Lemma 13.13 and Theorem 13.14] that for all sufficiently large n,

$$\mathtt{Pr}\left(\left\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : X_{\mathcal{M}}^n \text{ is } \epsilon_n\text{-recoverable from } \left(X_i^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right), Z_i^n\right), i \in \mathcal{M}\right\}\right) \geq 1 - \epsilon \quad (26)$$

provided $R_{\mathcal{M}} = (R_1, \ldots, R_m) \in \mathcal{R}(\mathcal{M}; Z_{\mathcal{M}})$, where ϵ_n vanishes exponentially rapidly in n. This assertion follows exactly as in the proof of [6, Proposition 1, with $A = \mathcal{M}$] but with $\tilde{X}_i$ there equal to (X_i, Z_i) rather than $X_i, i \in \mathcal{M}$. In particular, we shall choose $R_{\mathcal{M}} \in \mathcal{R}(\mathcal{M}; Z_{\mathcal{M}})$ such that

$$\sum_{i=1}^{m} R_i \leq R_{CO}(\mathcal{M}; Z_{\mathcal{M}}) + \frac{\delta}{2}. \quad (27)$$

Below we shall establish that

$$\Pr(\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : I\left(j_{\mathcal{M}}(X_{\mathcal{M}}^n) \wedge G^n\right) \geq \epsilon_n\}) \leq \epsilon' \quad (28)$$

for all n sufficiently large, to which end it suffices to show that

$$\mathtt{Pr}\left(\left\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : I\left(j_i(X_i^n) \wedge G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \geq \frac{\epsilon_n}{m}\right\}\right) \leq \frac{\epsilon'}{m}, \quad i \in \mathcal{M} \quad (29)$$

since

$$\begin{aligned} &I\left(j_{\mathcal{M}}\left(X_{\mathcal{M}}^n\right) \wedge G^n\right) \\ &\quad = \sum_{i=1}^{m} I\left(j_i\left(X_i^n\right) \wedge G^n \mid j_1\left(X_1^n\right), \ldots, j_{i-1}\left(X_{i-1}^n\right)\right) \\ &\quad \leq \sum_{i=1}^{m} I\left(j_i\left(X_i^n\right) \wedge G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right). \end{aligned}$$

Then it would follow from (26), (28) and definition of $Z_{\mathcal{M}}$ in (20) that

$$\mathtt{Pr}\left(\left\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : G^n \text{ is } \epsilon_n\text{-recoverable from } \left(X_i^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right), \quad i \in \mathcal{A}, \text{ and } I(j_{\mathcal{M}}(X_{\mathcal{M}}^n) \wedge G^n) < \epsilon_n\right\}\right) \geq 1 - \epsilon - \epsilon'.$$

This shows the existence of a particular realization $j_{\mathcal{M}}$ of $J_{\mathcal{M}}$ such that G^n is ϵ_n-SC from $\left(X_i^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right)$ for each $i \in \mathcal{A}$.

It now remains to prove (29). Fix $i \in \mathcal{M}$ and note that for each $j_i \in \mathcal{J}_i$, with $\|j_i\|$ denoting the cardinality of the (image) set $j_i(\mathcal{X}_i^n)$

$$\begin{aligned} &I\left(j_i\left(X_i^n\right) \wedge G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \\ &\quad \leq I\left(j_i\left(X_i^n\right) \wedge G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) + \log\|j_i\| \\ &\qquad - H\left(j_i\left(X_i^n\right)\right) \\ &\quad = D\left(j_i(X_i^n), \left(G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \,\middle\|\, U_{j_i(\mathcal{X}_i^n)} \times \left(G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right)\right) \end{aligned} \quad (30)$$

where the RHS above denotes the (Kullback-Leibler) divergence between the joint pmf of $j_i(X_i^n), \left(G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right)$ and the product of the uniform pmf on $j_i(\mathcal{X}_i^n)$ and the pmf of $\left(G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right)$. Using [6, Lemma 1], the RHS of (30) is bounded above further by

$$s_{var} \log \frac{\|j_i\|}{s_{var}} \quad (31)$$

where $s_{\text{var}} = s_{\text{var}}\left(j_i(X_i^n); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right)$ is the variational distance between the pmfs in the divergence above. Therefore, to prove (29), it suffices to show that

$$\mathtt{Pr}\left(\left\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : s_{var}\left(j_i(X_i^n); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \geq \frac{\epsilon_n}{m}\right\}\right) \leq \frac{\epsilon'}{m}, \quad i \in \mathcal{M} \quad (32)$$

on account of the fact that $\log\|j_i(X_i^n)\| = O(n)$, and the exponential decay to 0 of ϵ_n. Defining

$$\tilde{\mathcal{J}}_i = \left\{j_{\mathcal{M}\setminus\{i\}} \in \mathcal{J}_{\mathcal{M}\setminus\{i\}} : X_{\mathcal{M}}^n \text{ is } \epsilon_n\text{-recoverable from } \left(X_i^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right), Z_i^n\right)\right\}$$

we have by (26) that $\Pr(J_{\mathcal{M}\setminus\{i\}} \in \tilde{\mathcal{J}}_i) \geq 1 - \epsilon$. It follows that

$$\begin{aligned} &\mathtt{Pr}\left(\left\{j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}} : s_{var}\left(j_i\left(X_i^n\right); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \geq \frac{\epsilon_n}{m}\right\}\right) \\ &\leq \epsilon + \sum_{j_{\mathcal{M}\setminus\{i\}} \in \tilde{\mathcal{J}}_i} \Pr(J_{\mathcal{M}\setminus\{i\}} = j_{\mathcal{M}\setminus\{i\}}) \times \\ &\mathtt{Pr}\left(\left\{j_i \in \mathcal{J}_i : s_{\text{var}}\left(j_i(X_i^n); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \geq \frac{\epsilon_n}{m}\right\}\right) \end{aligned}$$

since J_i is independent of $J_{\mathcal{M}\setminus\{i\}}$. Thus, (32), and hence (29), will follow upon showing that

$$\mathtt{Pr}\left(\left\{j_i \in \mathcal{J}_i : s_{\text{var}}\left(j_i(X_i^n); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X_{\mathcal{M}\setminus\{i\}}^n\right)\right) \geq \frac{\epsilon_n}{m}\right\}\right) \leq \frac{\epsilon'}{m} - \epsilon, \quad j_{\mathcal{M}\setminus\{i\}} \in \tilde{\mathcal{J}}_i \quad (33)$$

for all n sufficiently large. Fix $j_{\mathcal{M}\setminus\{i\}} \in \tilde{\mathcal{J}}_i$. We take recourse to Lemma C2 in Appendix C, and set $U = X^n_{\mathcal{M}}, U' = X^n_i, V = G^n, h = j_{\mathcal{M}\setminus\{i\}}$, and

$$\mathcal{U}_0 = \Big\{x^n_{\mathcal{M}} \in \mathcal{X}^n_{\mathcal{M}} : \\ x^n_{\mathcal{M}} = \psi_i\left(x^n_i, j_{\mathcal{M}\setminus\{i\}}\left(x^n_{\mathcal{M}\setminus\{i\}}\right), g^n\left(x^n_{\mathcal{M}}\right)\mathbf{1}\left(i \in \mathcal{A}^c\right)\right)\Big\}$$

for some mapping ψ_i. By the definition of $\tilde{\mathcal{J}}_i$

$$\Pr(U \in \mathcal{U}_0) \geq 1 - \epsilon_n$$

so that condition (C2) (i) preceding Lemma C2 is met. Condition (C2) (ii), too, is met since conditioned on the events in (C2) (ii), only those $x^n_{\mathcal{M}} \in \mathcal{U}_0$ can occur that are determined uniquely by their i^{th} components x^n_i.

Upon choosing

$$d = \exp\left[n\left(H(X_{\mathcal{M}}|G) - \frac{\delta}{6}\right)\right],$$

in (C3), the hypotheses of Lemma C2 are satisfied with $\lambda = \sqrt{\epsilon_n}$ for an appropriate exponentially vanishing ϵ_n. Then, by Lemma C2, with

$$r = \lceil \exp[nR_i] \rceil, \quad r' = \left\lceil \exp\left[n\left(\sum_{l\in\mathcal{M}\setminus\{i\}} R_l + \frac{\delta}{6}\right)\right]\right\rceil,$$

and with J_i in the role of ϕ, we get from (C4) and (27) that

$$\mathtt{Pr}\left(\left\{j_i \in \mathcal{J}_i : s_{var}\left(j_i(X^n_i); G^n, j_{\mathcal{M}\setminus\{i\}}\left(X^n_{\mathcal{M}\setminus\{i\}}\right)\right) \geq 14\sqrt{\epsilon_n}\right\}\right)$$

decays to 0 doubly exponentially in n, which proves (33). This completes the proof of Theorem 5. □

B. Proof of Proposition 6

(i) Since the rv $(K^{(n)}_g, G^n)$, with nearly independent components, constitutes an ASK for $\mathcal{M}$ with side information $Z_{\mathcal{M}}$ as in (20), it is clear that

$$H(G) + C^g(\mathcal{M}; Z_{\mathcal{M}}) \leq C(\mathcal{M}; Z_{\mathcal{M}}). \tag{34}$$

In order to prove the reverse of (34), we show that $C(\mathcal{M}; Z_{\mathcal{M}}) - H(G)$ is an achievable ASK rate for K_g that additionally satisfies (25). First, note that in the proof of Theorem 5, the assertions (26) and (29) mean that for all sufficiently large n, there exists a public communication $F_{\mathcal{M}}$, say, such that $I(F_{\mathcal{M}} \wedge G^n) < \epsilon_n$ and $X^n_{\mathcal{M}}$ is ϵ_n-recoverable from $(X^n_i, F_{\mathcal{M}}, Z^n_i)$ for every $i \in \mathcal{M}$, with $\lim_n \epsilon_n = 0$. Fix $0 < \tau < \delta$, where δ is as in the proof of Theorem 5. Apply Lemma C2, choosing

$$U = U' = X^n_{\mathcal{M}}, \quad \mathcal{U}_0 = \mathcal{X}^n_{\mathcal{M}}, \quad V = G^n, \quad h = F_{\mathcal{M}}, \\ d = \exp\left[n\left(H\left(X_{\mathcal{M}}|G\right) - \frac{\tau}{6}\right)\right], \tag{35}$$

whereby the hypothesis (C2) of Lemma C2 is satisfied for all n sufficiently large. Fixing

$$r' = \left\lceil \exp\left[n\left(R_{CO}\left(\mathcal{M}; Z_{\mathcal{M}}\right) + \frac{\tau}{2}\right)\right]\right\rceil,$$

by Lemma C2 a randomly chosen ϕ of rate

$$\frac{1}{n}\log r = H(X_{\mathcal{M}}\,|\,G) - R_{CO}\left(\mathcal{M}; Z_{\mathcal{M}}\right) - \tau \\ = C\left(\mathcal{M}; Z_{\mathcal{M}}\right) - H(G) - \tau$$

will yield an ASK $K_g = K^{(n)}_g = \phi\left(X^n_{\mathcal{M}}\right)$ which is nearly independent of $(F_{\mathcal{M}}, G^n)$ (and, in particular, satisfies (25)) with positive probability, for all n sufficiently large.

(ii) The proof can be completed as that of part (i) upon showing that for a securely computable g, for all $\tau > 0$ and n sufficiently large, there exists a public communication $F'_{\mathcal{M}}$ that meets the following requirements: its rate does not exceed $R_{CO}(\mathcal{A}) + \tau$; $I(F'_{\mathcal{M}} \wedge G^n) < \epsilon_n$; and $X^n_{\mathcal{M}}$ is ϵ_n-recoverable from $(X^n_i, F'_{\mathcal{M}})$ for every $i \in \mathcal{A}$. To that end, for $R_{\mathcal{M}} = (R_1, \ldots, R_m) \in \mathcal{R}(\mathcal{M}; Z_{\mathcal{M}})$ as in the proof of Theorem 5, consider $R'_{\mathcal{M}} = (R'_1, \ldots, R'_m) \in \mathcal{R}(\mathcal{A})$ that satisfies $R'_i \leq R_i$ for all $i \in \mathcal{M}$ and

$$\sum_{i=1}^m R'_i \leq R_{CO}(\mathcal{A}) + \tau,$$

noting that $\mathcal{R}\left(\mathcal{M}; Z_{\mathcal{M}}\right) \subseteq \mathcal{R}(\mathcal{A})$. Further, for $J_{\mathcal{M}}$ and $\mathcal{J}_{\mathcal{M}}$ as in that proof, define a (map-valued) rv J'_i that is uniformly distributed on the family $\mathcal{J}'_i$ of all mappings from $\{1, \ldots, \lceil \exp(nR_i) \rceil\}$ to $\{1, \ldots, \lceil \exp(nR'_i) \rceil\}$, $i \in \mathcal{M}$. The rvs $J_1, \ldots, J_m, J'_1, \ldots, J'_m, X^n_{\mathcal{M}}$ are taken to be mutually independent. Define $\mathcal{J}^0_{\mathcal{M}}$ as the set of mappings $j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}}$ for which there exists a $j'_{\mathcal{M}} \in \mathcal{J}'_{\mathcal{M}}$ such that $X^n_{\mathcal{M}}$ is ϵ_n-recoverable from $(X^n_i, j'_{\mathcal{M}}\left(j_{\mathcal{M}}\left(X^n_{\mathcal{M}}\right)\right))$ for every $i \in \mathcal{A}$. By the general source network coding theorem [3, Lemma 13.13 and Theorem 13.14], applied to the random mapping $J'_{\mathcal{M}}\left(J_{\mathcal{M}}\right)$, it follows that for all sufficiently large n,

$$\Pr\left(J_{\mathcal{M}} \in J^0_{\mathcal{M}}\right) \geq 1 - \epsilon.$$

This, together with (26) and (29) in the proof of Theorem 5, imply that for a securely computable g there exist $j_{\mathcal{M}} \in \mathcal{J}_{\mathcal{M}}$ and $j'_{\mathcal{M}} \in \mathcal{J}'_{\mathcal{M}}$ for which the public communication $F'_{\mathcal{M}} \triangleq j'_{\mathcal{M}}(j_{\mathcal{M}})$ satisfies the aforementioned requirements. Finally, apply Lemma C2 with $U, U', \mathcal{U}_0, V$ and d as in (35) but with $h = F'_{\mathcal{M}}$ and

$$r' = \left\lceil \exp\left[n\left(R_{CO}\left(\mathcal{A}\right) + \frac{\tau}{2}\right)\right]\right\rceil.$$

As in the proof above of part (i), an SK $K'_g = K^{\prime(n)}_g$ of rate

$$\frac{1}{n}\log r = H(X_{\mathcal{M}}|G) - R_{CO}\left(\mathcal{A}\right) - \tau = C\left(\mathcal{A}\right) - H(G) - \tau$$

which is nearly independent of $(F'_{\mathcal{M}}, G^n)$ (and, hence, satisfies (25)) exists for all n sufficiently large. □

V. Discussion

We obtain simple necessary and sufficient conditions for secure computability expressed in terms of function entropy and ASK capacity. The latter is the largest rate of an SK for a new model in which side information is provided for use in only the recovery stage of SK generation. This model could be of independent interest. In particular, a function is securely computable if its entropy is less than the ASK capacity of an associated secrecy model. The difference is shown to correspond to the maximum achievable rate of an ASK which is independent of the securely computed function and, together with it, forms an ASK of optimum rate. Also, a function that is securely computed by $\mathcal{A}$ can be augmented to form an SK for $\mathcal{A}$ of maximum rate.

Our results extend trivially to functions defined on a block of symbols of *fixed* length in an obvious manner by considering larger alphabets composed of supersymbols of such length. However, they do not cover sequences of functions of symbols of increasing length (in n), e.g., a running average (in n).

In our proof of Theorem 5, g was securely computed from omniscience at all the terminals in $\mathcal{A} \subseteq \mathcal{M}$ that was attained using noninteractive public communication. However, omniscience is not necessary for the secure computation of g, and it is possible to make do with communication of rate less than $R_{CO}(\mathcal{A})$ using an interactive protocol. A related unresolved question is: What is the minimum rate of public communication for secure computation?

A natural generalization of the conditions for secure computability of g by $\mathcal{A} \subseteq \mathcal{M}$ given here entails a characterization of conditions for the secure computability of multiple functions $g_1, \ldots, g_k$ by subsets $\mathcal{A}_1, \ldots, \mathcal{A}_k$ of $\mathcal{M}$, respectively. This unsolved problem, in general, will not permit omniscience for any $\mathcal{A}_i, i = 1, \ldots, k$. For instance with $m = 2$, $\mathcal{A}_1 = \{1\}$, $\mathcal{A}_2 = \{2\}$, and X_1 and X_2 being independent, the functions $g_i(x_i) = x_i$, $i = 1, 2$, are securely computable trivially, but not through omniscience since, in this example, public communication is forbidden for the secure computation of g_1, g_2.

Yet another direction involves a model in which the terminals in $\mathcal{M}$ securely compute $G = g(X_{\mathcal{M}})$, and the eavesdropper has additional access to correlated side information that may not be available to the terminals in $\mathcal{M}$. Specifically, the eavesdropper observes n i.i.d. repetitions Z^n of a $\mathcal{Z}$-valued rv Z that has a given joint pmf with $X_{\mathcal{M}}$, in addition to the public communication $\mathbf{F}$ of the terminals in $\mathcal{M}$. The secrecy condition (3) is replaced by

$$I(G^n \wedge \mathbf{F} \mid Z^n) \leq \epsilon_n \tag{36}$$

noting that G need not be independent of Z. Having computed g securely, the terminals in $\mathcal{M}$ can extract a rv $K = K(G^n)$, of rate $H(G \mid Z)$, that is (nearly) independent of Z^n. Together with (36), this means that K is similarly independent of $(\mathbf{F}, Z^n)$. Since K constitutes a "wiretap secret key" (WSK), its rate $H(G \mid Z)$ necessarily cannot exceed the corresponding WSK capacity [15], [1], [6]. A single-letter characterization of WSK capacity remains unresolved in general (cf. [10]). The sufficiency of the previous necessary condition is unclear even when WSK capacity is known. In the special circumstance in which the terminals in $\mathcal{M}$, too, have access to Z^n, a single-letter characterization of WSK capacity is known [6]. In this case, our proof technique shows that the aforementioned necessary condition is also sufficient.

Appendix A

The proof of Lemma 3 is based on [8, Lemma, Sect. 4], which is paraphrased first. Let the rvs Q and R take values in the finite set $\mathcal{Q}$ and $\mathcal{R}$, respectively. For a stochastic matrix $W : \mathcal{Q} \to \mathcal{Q}$, let $\{\tilde{\mathcal{D}}_1, \ldots, \tilde{\mathcal{D}}_l\}$ be the ergodic decomposition (into communicating classes) (cf. e.g., [13]) of $\mathcal{Q}$ based on W. Let $\tilde{\mathcal{D}}^{(n)}$ denote a fixed ergodic class of $\mathcal{Q}^n$ (the n-fold Cartesian product of $\mathcal{Q}$) on the basis of W^n (the n-fold product of W). Let $\mathcal{D}^{(n)}$ and $\mathcal{R}^{(n)}$ be any (nonempty) subsets of $\tilde{\mathcal{D}}^{(n)}$ and $\mathcal{R}^n$, respectively.

Lemma GK: [8] For $\tilde{\mathcal{D}}^{(n)}, \mathcal{D}n, \mathcal{R}n$ as above, assume that

$$\begin{aligned} \Pr(Q^n \in \mathcal{D}n \mid R^n \in \mathcal{R}n) &\geq \exp[-n\epsilon_n], \\ \Pr(R^n \in \mathcal{R}n \mid Q^n \in \mathcal{D}n) &\geq \exp[-n\epsilon_n], \end{aligned} \tag{A1}$$

where $\lim_n \epsilon_n = 0$. Then (as stated in [8, bottom of p. 157])

$$\frac{\Pr\left(Q^n \in \mathcal{D}^{(n)}\right)}{\Pr\left(Q^n \in \tilde{\mathcal{D}}^{(n)}\right)} \geq \exp[-n\kappa\epsilon_n \log^2 \epsilon_n] \tag{A2}$$

for a (positive) constant κ that depends only on the pmf of (Q, R) and on W.

A simple consequence of (A2) is that for a given ergodic class $\tilde{\mathcal{D}}^{(n)}$ and disjoint subsets $\mathcal{D}_1^{(n)}, \ldots, \mathcal{D}_t^{(n)}$ of it, and subsets $\mathcal{R}_1^{(n)}, \ldots, \mathcal{R}_t^{(n)}$ (not necessarily distinct) of $\mathcal{R}^n$, such that $\mathcal{D}_{t'}^{(n)}, \mathcal{R}_{t'}^{(n)}, t' = 1, \ldots, t$, satisfy (A1), it holds that

$$t \leq \exp[n\kappa\epsilon_n \log^2 \epsilon_n]. \tag{A3}$$

Note that the ergodic decomposition of Q^n on the basis of W^n for the specific choice

$$W(q|q') = \sum_{r \in \mathcal{R}} \Pr(Q = q \mid R = r)\Pr(R = r \mid Q = q'), \quad q, q' \in \mathcal{Q}$$

corresponds to the set of values of $\mathtt{mcf}^n(Q, R)$ defined by (15) [8]. Next, pick $Q = Q_m$, $R = (Q_1, \ldots, Q_{m-1})$, and define the stochastic matrix $W : \mathcal{Q} \to \mathcal{Q}$ by

$$\begin{aligned} W(q|q') = \sum_{\alpha} &\Pr(Q = q \mid \mathtt{mcf}(Q_1, \ldots, Q_{m-1}) = \alpha) \times \\ &\Pr(\mathtt{mcf}(Q_1, \ldots, Q_{m-1}) = \alpha \mid Q = q'), \quad q, q' \in \mathcal{Q}. \end{aligned} \tag{A4}$$

The ergodic decomposition of $\mathcal{Q}^n$ on the basis of W^n (with W as in (A4)) will correspond to the set of values of $\mathtt{mcf}^n(Q_1, \ldots, Q_m)$, recalling (14). Since $\xi^{(n)}$ is ϵ-recoverable from $Q_i^n, i = 1, \ldots, m$, note that

$$\xi'^{(n)} = \left(\xi^{(n)}, \mathtt{mcf}^n(Q_1, \ldots, Q_m)\right)$$

also is ϵ-recoverable in the same sense, recalling Definition 7. This implies the existence of mappings $\xi_i'^{(n)}, i = 1, \ldots, m$, satisfying

$$\Pr\left(\xi_1'^{(n)}(Q_1^n) = \cdots = \xi_m'^{(n)}(Q_m^n) = \xi'^{(n)}\right) \geq 1 - \epsilon. \tag{A5}$$

For each fixed value $c = (c_1, c_2)$ of $\xi'^{(n)}$, let

$$\mathcal{D}_c^{(n)} = \left\{ q_m^n \in \mathcal{Q}_m^n : \xi_m'^{(n)}(q_m^n) = c \right\},$$
$$\mathcal{R}_c^{(n)} = \left\{ \left(q_1^n, \ldots, q_{m-1}^n\right) \in \mathcal{Q}_1^n \times \cdots \times \mathcal{Q}_{m-1}^n : \xi_i'^{(n)}\left(q_i^n\right) = c, i = 1, \ldots, m-1 \right\}.$$

Let $C(\epsilon)$ denote the set of c's such that

$$\Pr(Q^n \in \mathcal{D}_c^{(n)} \mid R^n \in \mathcal{R}_c^{(n)}) \geq 1 - \sqrt{\epsilon},$$
$$\Pr(R^n \in \mathcal{R}_c^{(n)} \mid Q^n \in \mathcal{D}_c^{(n)}) \geq 1 - \sqrt{\epsilon}. \tag{A6}$$

Then, as in [8, Proposition 1], it follows from (A5) that

$$\Pr\left(\xi'^{(n)} \in C(\epsilon)\right) \geq 1 - 4\sqrt{\epsilon}. \tag{A7}$$

Next, we observe for each fixed c_2, that the disjoint sets $\mathcal{D}_{c_1,c_2}^{(n)}$ lie in a fixed ergodic class of $\mathcal{Q}^n$ (determined by c_2). Since (A6) are compatible with the assumption (A1) for all n sufficiently large, we have from (A3) that

$$\|\{c_1 : (c_1, c_2) \in C(\epsilon)\}\| \leq \exp[n\kappa\epsilon_n \log^2 \epsilon_n], \tag{A8}$$

where κ depends on the pmf of $(Q_1, \ldots, Q_m)$ and W in (A4), and where $\lim_n \epsilon_n = 0$. Finally

$$\begin{aligned}
&\frac{1}{n} H\left(\xi'^{(n)}\right) = \frac{1}{n} H\left(\xi^{(n)}, \mathtt{mcf}^n(Q_1, \ldots, Q_m)\right) \\
&\leq H\left(\mathtt{mcf}(Q_1, \ldots, Q_m)\right) \\
&\quad + \frac{1}{n} H\left(\xi^{(n)}, \mathbf{1}\left(\xi'^{(n)} \in C(\epsilon)\right) \mid \mathtt{mcf}^n(Q_1, \ldots, Q_m)\right) \\
&\leq H\left(\mathtt{mcf}(Q_1, \ldots, Q_m)\right) + \frac{1}{n} \\
&\quad + \frac{1}{n} H\left(\xi^{(n)} \mid \mathtt{mcf}^n(Q_1, \ldots, Q_m), \mathbf{1}\left(\xi'^{(n)} \in C(\epsilon)\right)\right) \\
&\leq H(\mathtt{mcf}(Q_1, \ldots, Q_m)) + \delta_n
\end{aligned}$$

where $\lim_n \delta_n = 0$ by (A7) and (A8). □

Appendix B

Considering first the achievability part, fix $\delta > 0$. From the result for a general source network [3, Theorem 13.14] it follows, as in the proof of [6, Prop. 1], that for $R_{\mathcal{M}} \in \mathcal{R}\left(\mathcal{A}', Z_{\mathcal{A}'}\right)$ and all n sufficiently large, there exists a noninteractive communication $\mathbf{F}^{(n)} = (F_1^{(n)}, \ldots, F_m^{(n)})$ with

$$\frac{1}{n} \log \left\| \mathbf{F}^{(n)} \right\| \leq \sum_{i=1}^m R_i + \delta$$

such that $\mathcal{X}_{\mathcal{M}}^n$ is ϵ_n-recoverable from $\left(X_i^n, Z_i^n, \mathbf{F}^{(n)}\right), i \in \mathcal{A}'$. Therefore, $\left\{\mathtt{mcf}\left((X_{\mathcal{M}t}, Z_{it})_{i \in A'}\right)\right\}_{t=1}^n$ is ϵ_n-recoverable from $\left(X_i^n, Z_i^n, \mathbf{F}^{(n)}\right), i \in \mathcal{A}'$. The last step takes recourse to Lemma C2 in Appendix C. Specifically, choose $U = U' = \left\{\mathtt{mcf}\left((X_{\mathcal{M}t}, Z_{it})_{i \in A'}\right)\right\}_{t=1}^n, \mathcal{U}_0 = \mathcal{U}$, $V =$ constant, $h = \mathbf{F}^{(n)}$, $d = n\left[H\left(\mathtt{mcf}\left((X_{\mathcal{M}}, Z_i)_{i \in A'}\right)\right) - \delta\right]$, whereby the hypothesis (C2) of Lemma C2 is satisfied for all n sufficiently large. Fixing

$$r' = \left\lceil \exp\left[n \left(\sum_{i=1}^m R_i + \delta \right) \right] \right\rceil$$

Lemma C2 implies the existence of a ϕ, and thereby an ASK $K^{(n)} = \phi\left(\left\{\mathtt{mcf}\left((X_{\mathcal{M}t}, Z_{it})_{i \in A'}\right)\right\}_{t=1}^n\right)$, of rate

$$\frac{1}{n} \log r = H\left(\mathtt{mcf}\left((X_{\mathcal{M}}, Z_i)_{i \in A'}\right)\right) - \sum_{i=1}^m R_i - 3\delta.$$

In particular, we can choose

$$\sum_{i=1}^m R_i \leq R_{CO}\left(\mathcal{A}'; Z_{\mathcal{A}'}\right) + \frac{\delta}{2}.$$

Since δ was arbitrary, this establishes the achievability part.

We shall establish a stronger converse result by requiring the ASK as in Definition 5 to satisfy the weaker secrecy condition (7), or by allowing the ASK to depend explicitly on the randomization $U_{\mathcal{M}}$ but enforcing the strong secrecy condition (3). Let $K = K^{(n)}\left(U_{\mathcal{M}}, X_{\mathcal{M}}^n, Z_{\mathcal{A}'}^n\right)$ be an ϵ_n-ASK for $\mathcal{A}'$, achievable using observations of length n, randomization $U_{\mathcal{M}}$, public communication $\mathbf{F} = \mathbf{F}\left(U_{\mathcal{M}}, X_{\mathcal{M}}^n\right)$ and side information $Z_{\mathcal{A}'}^n$. Then, by (7)

$$\frac{1}{n} H(K) \leq \frac{1}{n} H(K \mid \mathbf{F}) + \epsilon_n. \tag{B1}$$

Let $K_u = K\left(u, X_{\mathcal{M}}^n, Z_{\mathcal{A}'}^n\right)$ denote the random value of the ASK for a fixed $U_{\mathcal{M}} = u$. Since $(X_{\mathcal{M}}^n, K)$ is ϵ_n-recoverable from the rvs $(U_{\mathcal{M}}, X_{\mathcal{M}}^n, Z_i^n)$ for each $i \in \mathcal{A}'$,

$$\begin{aligned}
\mathtt{P}_{U_{\mathcal{M}}}\big(\{u : &(X_{\mathcal{M}}^n, K_u) \text{ is } \sqrt{\epsilon_n}\text{-recoverable from} \\
&(U_{\mathcal{M}} = u, X_{\mathcal{M}}^n, Z_i^n) \text{ for each } i \in \mathcal{A}'\}\big) \\
&\geq 1 - \sqrt{\epsilon_n}.
\end{aligned} \tag{B2}$$

Also, for each $U_{\mathcal{M}} = u$

$$\frac{1}{n} H\left(X_{\mathcal{M}}^n, K \mid U_{\mathcal{M}} = u\right) = \frac{1}{n} H\left(X_{\mathcal{M}}^n, K_u\right)$$

by the independence of $U_{\mathcal{M}}$ and $(X_{\mathcal{M}}^n, Z_{\mathcal{A}'}^n)$, and therefore, by Lemma 3, for u in the set in (B2),

$$\frac{1}{n} H\left(X_{\mathcal{M}}^n, K \mid U_{\mathcal{M}} = u\right) \leq H\left(\mathtt{mcf}\left((X_{\mathcal{M}}, Z_i)_{i \in \mathcal{A}'}\right)\right) + \delta_n, \tag{B3}$$

for all n sufficiently large and where $\lim_n \delta_n = 0$. Then,

$$\begin{aligned}
&\frac{1}{n} H(U_{\mathcal{M}}, X_{\mathcal{M}}^n, K) \\
&\quad \leq \frac{1}{n} H\left(U_{\mathcal{M}}\right) + H\left(\mathtt{mcf}\left((X_{\mathcal{M}}, Z_i)_{i \in \mathcal{A}'}\right)\right) + \delta_n \\
&\qquad + \sqrt{\epsilon_n} \log\left(|\mathcal{X}_{\mathcal{M}}||\mathcal{Z}_{\mathcal{A}'}|\right),
\end{aligned} \tag{B4}$$

by (B2) and (B3). The proof is now completed along the lines of [6, Lemma 2 and Theorem 3]. Specifically, denoting the set of positive integers $\{1,\dots,l\}$ by $[1,l]$,

$$\frac{1}{n}H(U_{\mathcal{M}},X_{\mathcal{M}}^n,K)=\frac{1}{n}H(K\mid\mathbf{F})+\sum_{i=1}^{m}R_i'+\frac{1}{n}H(U_{\mathcal{M}})$$

where

$$R_i'=\frac{1}{n}\sum_{\nu:\nu\equiv i \bmod m}H(F_\nu\mid F_{[1,\nu-1]})+\frac{1}{n}H\left(U_i,X_i^n\mid\mathbf{F},K,U_{[1,i-1]},X_{[1,i-1]}^n\right)-H(U_i). \tag{B5}$$

Consider $B\subsetneq\mathcal{M}$, $\mathcal{A}'\nsubseteq B$. For $j\in\mathcal{A}'\cap B^c$, we have

$$\begin{aligned}&\frac{1}{n}H\left(U_B\right)+\frac{1}{n}H\left(X_B\mid X_{B^c}^n,Z_j^n\right)\\&=\frac{1}{n}H\left(U_B,X_B^n\mid U_{B^c},X_{B^c}^n,Z_j^n\right)\\&=\frac{1}{n}H\left(F_1,\dots,F_{rm},K,U_B,X_B^n\mid U_{B^c},X_{B^c}^n,Z_j^n\right).\end{aligned}$$

Furthermore, since K is ϵ_n-recoverable from $(\mathbf{F},U_{B^c},X_{B^c}^n,Z_j^n)$ and $H(F_\nu|U_{B^c},X_{B^c}^n)=0$ for $\nu\equiv i \bmod m$ with $i\in B^c$,

$$\begin{aligned}&\frac{1}{n}H\left(F_1,\dots,F_{rm},K,U_B,X_B^n\mid U_{B^c},X_{B^c}^n,Z_j^n\right)\\&=\frac{1}{n}\sum_{\nu=1}^{rm}H\left(F_\nu\mid F_{[1,\nu-1]},U_{B^c},X_{B^c}^n,Z_j^n\right)\\&\quad+\frac{1}{n}H\left(K\mid U_{B^c},X_{B^c}^n,Z_j^n,\mathbf{F}\right)\\&\quad+\frac{1}{n}\sum_{i\in B}H\Big(U_i,X_i^n\mid U_{B^c\cap[i+1,m]},X_{B^c\cap[i+1,m]}^n,Z_j^n,\\&\qquad\qquad\mathbf{F},K,U_{[1,i-1]},X_{[1,i-1]}^n\Big)\\&\le\frac{1}{n}\sum_{i\in B}\left[\sum_{\nu:\nu\equiv i \bmod m}H\left(F_\nu\mid F_{[1,\nu-1]}\right)+\right.\\&\qquad\left.H\left(U_i,X_i^n\mid\mathbf{F},K,U_{[1,i-1]},X_{[1,i-1]}^n\right)\right]\\&\quad+\frac{\epsilon_n\log|\mathcal{K}|+1}{n}\\&\le\sum_{i\in B}R_i+H(U_B)\end{aligned}\tag{B6}$$

where

$$R_i\triangleq\left(R_i'+\frac{\epsilon_n\log|\mathcal{K}|+1}{n}\right),\quad i\in\mathcal{M}.$$

It follows from (B1) and (B4)–(B6) that

$$\frac{1}{n}H(K)\le H\left(\mathtt{mcf}\left((X_{\mathcal{M}},Z_i)_{i\in\mathcal{A}'}\right)\right)-\sum_{i=1}^{m}R_i+\epsilon_n+\delta_n+\frac{\epsilon_n\log|\mathcal{K}|+1}{n}+\sqrt{\epsilon_n}\log\left(|\mathcal{X}_{\mathcal{M}}||\mathcal{Z}_{\mathcal{A}'}|\right), \tag{B7}$$

where $R_{\mathcal{M}}\in\mathcal{R}\left(\mathcal{A}',Z_{\mathcal{A}'}\right)$ from (B6), and therefore

$$\sum_{i=1}^{m}R_i\ge R_{CO}\left(\mathcal{A}',Z_{\mathcal{A}'}\right). \tag{B8}$$

Then, (B7), (B8) imply

$$\frac{1}{n}H(K)\le C\left(\mathcal{A}',Z_{\mathcal{A}'}\right)+\epsilon_n+\delta_n+\frac{\epsilon_n\log|\mathcal{K}|+1}{n}+\sqrt{\epsilon_n}\log\left(|\mathcal{X}_{\mathcal{M}}||\mathcal{Z}_{\mathcal{A}'}|\right). \tag{B9}$$

If $K=K\left(X_{\mathcal{M}}^n,Z_{\mathcal{A}'}^n\right)$ as in Definition 5, then $|\mathcal{K}|\le\left(|\mathcal{X}||\mathcal{Z}_{\mathcal{A}'}|\right)^n$ and the converse part follows from (B9). On the other hand, for $K=K\left(U_{\mathcal{M}},X_{\mathcal{M}}^n,Z_{\mathcal{A}'}^n\right)$, the proof is completed using (3) in the manner of [6, Theorem 3]. This completes the converse part. □

APPENDIX C

Our proof of achievability in Theorem 4 and sufficiency in Theorem 5 rely on a "balanced coloring lemma" in [1]; we state a version of it from [6].

Lemma C1: [1, Lemma 3.1] Let $\mathcal{P}$ be any family of N pmfs on a finite set $\mathcal{U}$, and let $d>0$ be such that $P\in\mathcal{P}$ satisfies

$$P\left(\left\{u:P(u)>\frac{1}{d}\right\}\right)\le\epsilon \tag{C1}$$

for some $0<\epsilon<1/9$. Then the probability that a randomly selected mapping $\phi:\mathcal{U}\to\{1,\dots,r\}$ fails to satisfy

$$\sum_{i=1}^{r}\left|\sum_{u:\phi(u)=i}P(u)-\frac{1}{r}\right|<3\epsilon,$$

simultaneously for each $P\in\mathcal{P}$, is less than $2Nr\exp\left(-\frac{\epsilon^2 d}{3r}\right)$.

In contrast with the application of Lemma C1 in [6, Lemma B.2], our mentioned proofs call for a balanced coloring of a set corresponding to a rv that differs from another rv for which probability bounds are used. However, both rvs agree with high probability when conditioned on a set of interest.

Consider rvs U,U',V with values in finite sets $\mathcal{U},\mathcal{U}',\mathcal{V}$, respectively, where U' is a function of U, and a mapping $h:\mathcal{U}\to\{1,\dots,r'\}$. For $\lambda>0$, let $\mathcal{U}_0$ be a subset of $\mathcal{U}$ such that
(i) $\Pr(U\in\mathcal{U}_0)>1-\lambda^2$;
(ii) given the event $\{U\in\mathcal{U}_0,h(U)=j,U'=u',V=v\}$, there exists $u=u(u')\in\mathcal{U}_0$ satisfying

$$\begin{aligned}&\Pr(U'=u'\mid h(U)=j,V=v,U\in\mathcal{U}_0)\\&=\Pr(U=u\mid h(U)=j,V=v,U\in\mathcal{U}_0)\end{aligned}\tag{C2}$$

for $1\le j\le r'$ and $v\in\mathcal{V}$. Then the following holds.

Lemma C2: Let the rvs U,U',V and the set $\mathcal{U}_0$ be as above. Further, assume that

$$P_{UV}\left(\left\{(u,v):\Pr(U=u\mid V=v)>\frac{1}{d}\right\}\right)\le\lambda^2. \tag{C3}$$

Then, a randomly selected mapping $\phi : \mathcal{U}' \to \{1, \ldots, r\}$ fails to satisfy

$$\sum_{j=1}^{r'} \sum_{v \in \mathcal{V}} \Pr(h(U) = j, V = v) \times \sum_{i=1}^{r} \left| \sum_{\substack{u' \in \mathcal{U}': \\ \phi(u') = i}} \Pr(U' = u' \mid h(U) = j, V = v) - \frac{1}{r} \right| < 14\lambda \tag{C4}$$

with probability less than $2rr'|\mathcal{V}| \exp\left(-\frac{c\lambda^3 d}{rr'}\right)$ for a constant $c > 0$.

Proof: Using the condition (i) in the definition of $\mathcal{U}_0$, the left-hand side (LHS) of (C4) is bounded above by

$$2\lambda^2 + \sum_{j=1}^{r'} \sum_{v \in \mathcal{V}} \Pr(h(U) = j, V = v, U \in \mathcal{U}_0) \sum_{i=1}^{r} \left| \sum_{\substack{u' \in \mathcal{U}': \\ \phi(u') = i}} \Pr(U' = u' \mid h(U) = j, V = v, U \in \mathcal{U}_0) - \frac{1}{r} \right|.$$

Therefore, it is sufficient to prove that

$$\sum_{j=1}^{r'} \sum_{v \in \mathcal{V}} \Pr(h(U) = j, V = v, U \in \mathcal{U}_0) \sum_{i=1}^{r} \left| \sum_{\substack{u' \in \mathcal{U}': \\ \phi(u') = i}} \Pr(U' = u' \mid h(U) = j, V = v, U \in \mathcal{U}_0) - \frac{1}{r} \right| < 12\lambda \tag{C5}$$

with probability greater than $1 - 2rr'|\mathcal{V}| \exp\left(-\frac{c\lambda^3 d}{rr'}\right)$ for a constant $c > 0$.

Let

$$q = P_V\left(\left\{v \in \mathcal{V} : \Pr(U \in \mathcal{U}_0 | V = v) < \frac{1 - \lambda^2}{3}\right\}\right).$$

Then, since

$$\begin{aligned} 1 - \lambda^2 &\le \Pr(U \in \mathcal{U}_0) \\ &\le \sum_{\substack{v \in V: \\ \Pr(U \in \mathcal{U}_0 | V = v) < \frac{1-\lambda^2}{3}}} \Pr(U \in \mathcal{U}_0 | V = v) P_V(v) + (1 - q) \\ &< \frac{1 - \lambda^2}{3} q + (1 - q) \end{aligned}$$

we get from the extremities above that

$$q < \frac{3\lambda^2}{2}. \tag{C6}$$

For $u \in \mathcal{U}_0$ and $v \in \mathcal{V}$ satisfying

$$\Pr(U \in \mathcal{U}_0 | V = v) \ge \frac{1 - \lambda^2}{3}$$
$$\Pr(U = u | V = v, U \in \mathcal{U}_0) > \frac{3}{d(1 - \lambda^2)}$$

we have that

$$\Pr(U = u | V = v) > \frac{1}{d}.$$

Therefore, by (C6) and (C3), it follows that (see the first inequality at the bottom of the page), which is the same as

$$\sum_{j=1}^{r'} \sum_{v \in \mathcal{V}} \Pr(h(U) = j, V = v, U \in \mathcal{U}_0) \times \sum_{\substack{u \in \mathcal{U}_0: \\ \Pr(U = u | V = v, U \in \mathcal{U}_0) > \frac{3}{d(1-\lambda^2)}}} \Pr(U = u | h(U) = j, V = v, U \in \mathcal{U}_0) < \frac{5\lambda^2}{2}. \tag{C7}$$

The bound in (C7) will now play the role of [6, ineq. (50), p. 3059] and the remaining steps of our proof, which are parallel to those in [6, Lemma B.2], are provided here for completeness.

Setting D to be the set of those (j, v) that satisfy the second inequality at the bottom of the page, we get that

$$\sum_{(j,v) \in D^c} \Pr(h(U) = j, V = v, U \in \mathcal{U}_0) < \lambda. \tag{C8}$$

$$\sum_{\substack{(u,v): \\ u \in \mathcal{U}_0,\, \Pr(U = u | V = v, U \in \mathcal{U}_0) > \frac{3}{d(1-\lambda^2)}}} \Pr(U = u, V = v) \le \lambda^2 + q < \frac{5\lambda^2}{2}$$

$$\sum_{\substack{u \in \mathcal{U}: \\ \Pr(U = u | V = v, U \in \mathcal{U}_0) > \frac{3}{d(1-\lambda^2)}}} \Pr(U = u | h(U) = j, V = v, U \in \mathcal{U}_0) \le \frac{5\lambda}{2}$$

Next, defining

$$E = \Big\{(j,v) : \Pr(h(U)=j, V=v, U\in\mathcal{U}_0) \geq \frac{\lambda}{r'}\Pr(V=v, U\in\mathcal{U}_0)\Big\}$$

it holds for $(j,v)\in E$ that

$$\Pr(U=u|h(U)=j,V=v,U\in\mathcal{U}_0) \leq \frac{r'}{\lambda}\Pr(U=u|V=v,U\in\mathcal{U}_0). \tag{C9}$$

Also,

$$\begin{aligned}&\sum_{(j,v)\in E^c}\Pr(h(U)=j,V=v,U\in\mathcal{U}_0)\\ &< \frac{\lambda}{r'}\sum_{j=1}^{r'}\sum_{v\in\mathcal{V}}\Pr(V=v,U\in\mathcal{U}_0)\\ &\leq \lambda.\end{aligned} \tag{C10}$$

Further, for $(j,v)\in E$, if

$$\Pr(U=u|h(U)=j,V=v,U\in\mathcal{U}_0) > \frac{3r'}{\lambda d(1-\lambda^2)} \tag{C11}$$

then from (C9), we have

$$\Pr(U=u|V=v,U\in\mathcal{U}_0) > \frac{3}{d(1-\lambda^2)}. \tag{C12}$$

Therefore, denoting by $\mathcal{I}(j,v)$ the event $\{h(U)=j, V=v, U\in\mathcal{U}_0\}$, and recalling the conditions that define $\mathcal{U}_0$ in (C2), we have for $(j,v)\in E\cap D$ that

$$\begin{aligned}&\sum_{\substack{u'\in\mathcal{U}':\\ \Pr(U'=u'|\mathcal{I}(j,v))>\frac{3r'}{\lambda d(1-\lambda^2)}}}\Pr(U'=u'|\mathcal{I}(j,v))\\ &= \sum_{\substack{u'\in\mathcal{U}':\\ \Pr(U=u(u')|\mathcal{I}(j,v))>\frac{3r'}{\lambda d(1-\lambda^2)}}}\Pr(U=u(u')|\mathcal{I}(j,v))\\ &= \sum_{\substack{u\in\mathcal{U}:\\ \Pr(U=u|\mathcal{I}(j,v))>\frac{3r'}{\lambda d(1-\lambda^2)}}}\Pr(U=u|\mathcal{I}(j,v))\\ &\leq \frac{5\lambda}{2}\end{aligned} \tag{C13}$$

where the first equality is by (C2), the second equality is due to U' being a function of U, and the previous inequality is by (C11), (C12) and the definition of the set D. Also, using (C8), (C10), we get

$$\sum_{(j,v)\in E\cap D}\Pr(h(U)=j,V=v,U\in\mathcal{U}_0)\geq 1-2\lambda. \tag{C14}$$

Now, the LHS of (C5) is bounded, using (C14), as

$$\begin{aligned}&\sum_{j=1}^{r'}\sum_{v\in\mathcal{V}}\Pr(h(U)=j,V=v,U\in\mathcal{U}_0)\sum_{i=1}^{r}\\ &\left|\sum_{\substack{u'\in\mathcal{U}':\\ \phi(u')=i}}\Pr(U'=u'\mid h(U)=j,V=v,U\in\mathcal{U}_0)-\frac{1}{r}\right|\\ &\leq 4\lambda+\\ &\sum_{(j,v)\in E\cap D}\Pr(h(U)=j,V=v,U\in\mathcal{U}_0)\sum_{i=1}^{r}\\ &\left|\sum_{\substack{u'\in\mathcal{U}':\\ \phi(u')=i}}\Pr(U'=u'\mid h(U)=j,V=v,U\in\mathcal{U}_0)-\frac{1}{r}\right|.\end{aligned} \tag{C15}$$

Using (C13), the family of pmfs $\{\Pr(U'=(\,\cdot\,)|h(U)=j,V=v,U\in\mathcal{U}_0),\quad (j,v)\in E\cap D\}$ satisfies the hypothesis (C1) of Lemma C1 with d replaced by $\frac{\lambda(1-\lambda^2)d}{3r'}$ and ϵ replaced by $5\lambda/2$; assume that $0<\lambda<2/45$ so as to meet the condition following (C1). The mentioned family consists of at most $r'|\mathcal{V}|$ pmfs. Therefore, using Lemma C1,

$$\begin{aligned}&\sum_{j=1}^{r'}\sum_{v\in\mathcal{V}}\Pr(h(U)=j,V=v,U\in\mathcal{U}_0)\times\\ &\sum_{i=1}^{r}\left|\sum_{\substack{u'\in\mathcal{U}':\\ \phi(u')=i}}\Pr(U'=u'\mid h(U)=j,V=v,U\in\mathcal{U}_0)-\frac{1}{r}\right|\\ &<\frac{23\lambda}{2}\end{aligned}$$

with probability greater than

$$\begin{aligned}&1-2rr'|\mathcal{V}|\exp\left(-\frac{25\lambda^3(1-\lambda^2)d}{36rr'}\right)\\ &\geq 1-2rr'|\mathcal{V}|\exp\left(-\frac{c\lambda^3 d}{rr'}\right)\end{aligned}$$

for a constant c. This completes the proof of (C5), and thereby the lemma. □

ACKNOWLEDGMENT

The authors thank Sirin Nitinawarat for helpful discussions.

REFERENCES

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

[2] R. Ahlswede and I. Csiszár, "On the oblivious transfer capacity," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2007, pp. 2061–2064.

[3] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Channels*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press., 2011.
[4] I. Csiszár, "Almost independence and secrecy capacity," *Prob. Pered. Inf.* , vol. 32, no. 1, pp. 48–57, 1996.
[5] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, 2000.
[6] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.
[7] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, 2008.
[8] P. Gács and J. Körner, "Common information is far less than mutual information," *Probl. Contr. Inf. Theory*, vol. 2, no. 2, pp. 149–162, 1973.
[9] R. G. Gallager, "Finding parity in a simple broadcast network," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 176–180, 1988.
[10] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, 2010.
[11] A. Giridhar and P. Kumar, "Computing and communicating functions over sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 755–764, 2005.
[12] J. Korner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, 1979.
[13] M. Loeve, *Probability Theory*. New York: Van Nostrand, 1955, pp. 157, 28–42.
[14] N. Ma, P. Ishwar, and P. Gupta, "Information-theoretic bounds for multiround function computation in collocated networks," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2009, pp. 2306–2310.
[15] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, 1993.
[16] U. M. Maurer, *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut, Ed. *et al.* Norwell, MA: Kluwer, 1994, ch. 26, pp. 271–285.
[17] A. Nascimento and A. Winter, "On the oblivious transfer capacity of noisy correlations," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2009, pp. 1871–1875.
[18] A. Orlitsky and A. El Gamal, "Communication with secrecy constraints," in *Proc. ACM Symp. Theory of Comput. (STOC)*, 1984, pp. 217–224.
[19] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, 2001.
[20] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, pp. 2–10, 1974.
[21] A. C. Yao, "Some complexity questions related to distributive computing," in *Proc. ACM Symp. on Theory of Comput. (STOC)*, 1979, pp. 209–213.
[22] C. Ye, "Information Theoretic Generation of Multiple Secret Keys," Ph.D. thesis, Dept. Elect. and Comput. Eng., Univ. Maryland, College Park, 2005.
[23] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," in *Proc. Int. Symp. Inf. Theory*, 2005, pp. 2133–2137.
[24] C. Ye and P. Narayan, "Secret key and private constructions for simple multiterminal source models," *IEEE Trans. Inf. Theory*, accepted for publication.

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, in 2007.

He is currently a Ph.D. candidate at the University of Maryland, College Park.

Prakash Narayan (F'01) received the Bachelor of Technology degree in electrical engineering from the Indian Institute of Technology, Madras, in 1976. He received 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 a 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 currently serves as a Member of the Board of Governors of the IEEE Information Theory Society.

Piyush Gupta (F'11) received the Bachelor of Technology degree in electrical engineering from the Indian Institute of Technology, Bombay, in 1993, the Master of Science degree in computer science and automation from the Indian Institute of Science, Bangalore, in 1996, and the Ph.D. degree in electrical and computer engineering from the University of Illinois, Urbana-Champaign, in 2000.

From 1993 to 1994, he was a design engineer at the Center for Development of Telematics, Bangalore. Since September 2000, he has been a Member of Technical Staff in the Mathematics of Networks and Communications Research Department at Alcatel-Lucent, Bell Laboratories, Murray Hill, NJ. His research interests include wireless networks, network information theory, and learning and adaptive systems.