Function Computation Without Secure Links: Information and Leakage Rates

Rémi A. Chou
Department of Electrical Engineering & Computer Science
Wichita State University
Wichita, KS 67260
remi.chou@wichita.edu

Jörg Kliewer
Department of Electrical & Computer Engineering
New Jersey Institute of Technology
Newark, NJ 07102
jkliewer@njit.edu

2022 IEEE International Symposium on Information Theory (ISIT) | 978-1-6654-2159-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISIT50566.2022.9834387

***Abstract*—Consider L users, who each holds private data, and one fusion center who must compute a function of the private data of the L users. To accomplish this task, each user can make a single use of a public and noiseless broadcast channel. In this setting, and in the absence of any additional resources such as secure links, we study the optimal communication rates and minimum information leakages on the private user data that are achievable. Specifically, we study the information leakage of the user data at the fusion center (beyond the knowledge of the function output), as well as at predefined groups of colluding users who eavesdrop one another. We derive the capacity region when the user data is independent, and inner and outer regions for the capacity region when the user data is correlated.**

I. Introduction

In this paper, we consider a function computation setting where the users do not have access to secure links to communicate among them but only to a public and noiseless broadcast channel. This setting contrasts with traditional information-theoretically secure multiparty computation settings, e.g., [2] and references therein, where each pair of users has unlimited access to an information-theoretically secure communication link. Without this assumption, perfect information-theoretic security of user data is impossible to obtain for the computation of arbitrary functions. In this context, our goal is to (i) understand the level of privacy that is attainable, i.e., quantify the minimum information leakage on the private user data that is achievable, and (ii) determine optimal communication rates for the computation of arbitrary functions.

In our setting, we consider L users who each holds private data, and one fusion center who must compute a function of their data. Each user can send one message, i.e., an encoded version of their data, over the public and noiseless broadcast channel. We are then interested in characterizing the optimal communication rates, as well as the minimum information leakage on the private user data that is achievable. We distinguish two types of information leakage. The first one is the amount of information that the fusion center can learn from the public communication about the user data, beyond the knowledge of the function output. The second one is the amount of information that a group of colluding users can learn from the public communication about the data of all the other users. The private data of a given user is modeled by a sequence of independent and identically distributed random variables. We derive a capacity result when the data of the users is independent, and inner and outer regions for the capacity region when the data is correlated. We also derive a capacity result for the fully decentralized case where a designated user needs to compute the function instead of the fusion center.

Note that in the absence of any privacy or security constraints, several variants of function computation have been studied under the same model assumptions as in our setting, namely, (i) the inputs of the function are sequences of independent and identically distributed random variables, and (ii) communication links among users are noiseless, e.g., [3], [4]. More advanced settings for function computation have also considered interactive communication, e.g., [5]–[7]. Other works, e.g., [8], [9], have considered settings related to multiparty computation but with the additional assumptions that any pair of users can interactively communicate over secure noiseless links, and the additional requirement that no user data leakage is allowed. Specifically, [9] studies the minimum amount of randomness needed at the users to perform secure addition, and [8] studies optimal communication rates for function computation among three users – full characterization of such optimal communication rates have been established for the computation of a few functions but remains an open problem in general. Another line of work has focused on function computation models when no user data leakage is allowed but in the absence of secure links, e.g., [10], [11]. In such settings not all functions can be computed. Finally, the closest setting to our model in this paper is function computation with privacy constraints, which has also been studied under assumptions (i) and (ii) in [12]. The main differences between [12] and our work is that [12] focuses on the computation of functions with three inputs and considers a single external eavesdropper, whereas our model considers computation of functions with an arbitrary number of inputs and groups of colluding users eavesdrop one another.

II. Problem Statement

Consider L users indexed in $\mathcal{L} \triangleq [\![1, L]\!]$. Consider L finite alphabets $(\mathcal{X}_l)_{l\in\mathcal{L}}$ and a probability distribution $p_{X_\mathcal{L}}$ defined

This work was supported in part by NSF grants CCF-2201824 and CCF-2201825. Full proofs are available in [1].

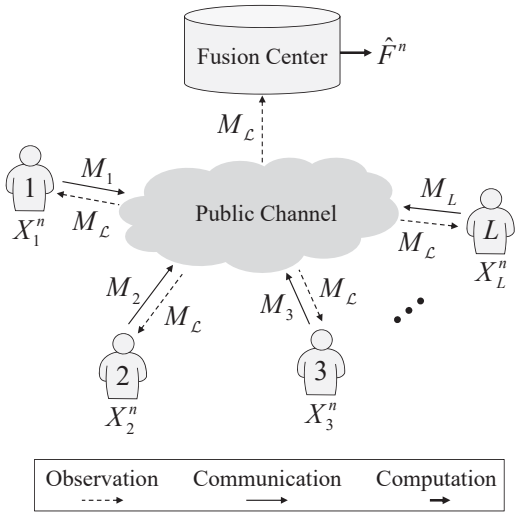

Fig. 1. Function computation over a public and noiseless broadcast channel. $M_{\mathcal{L}} \triangleq (M_l)_{l\in\mathcal{L}}$ and $\hat{F}^n$ is an estimate of $F^n \triangleq (f(X_{\mathcal{L},i}))_{i\in[\![1,n]\!]}$.

over $\mathcal{X}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}} \mathcal{X}_l$ with the notation $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$. Consider $X_{\mathcal{L}}^n$ distributed according to $\prod_{i=1}^n p_{X_{\mathcal{L}}}$ and the notation $X_{\mathcal{L}}^n \triangleq (X_{\mathcal{L},i})_{i\in[\![1,n]\!]}$. Assume that X_l^n corresponds to an input available at User $l \in \mathcal{L}$. For a function $f : \mathcal{X}_{\mathcal{L}} \to \mathcal{F}$, define $F \triangleq f(X_{\mathcal{L}})$, $F^n \triangleq (f(X_{\mathcal{L},i}))_{i\in[\![1,n]\!]}$, and assume that this function needs to be computed at a fusion center. Assume that there is a public and noiseless broadcast channel from the users to the fusion center. Finally, let $\mathbb{A}$ be an arbitrary and fixed set of non-empty, possibly overlapping, subsets of users, such that any set of colluding users $\mathcal{A} \in \mathbb{A}$ is interested in learning the inputs of the other users in $\mathcal{A}^c$ from the public communication. For instance, if $L = 3$ and $\mathbb{A} \triangleq \{\{1, 2\}, \{2, 3\}\}$, then Users 1 and 2 (resp. 2 and 3) could be interested in colluding to learn information about the private data of User 3 (resp. 1). The setting is depicted in Figure 1.

Definition 1. *A $((2^{nR_l})_{l\in\mathcal{L}}, n)$ computation scheme consists of*

- *L messages sets $\mathcal{M}_l \triangleq [\![1, 2^{nR_l}]\!]$, $l \in \mathcal{L}$;*
- *L encoding functions $e_l : \mathcal{X}_l^n \to \mathcal{M}_l$, $l \in \mathcal{L}$;*
- *One decoding function $d : \mathcal{M}_{\mathcal{L}} \to \mathcal{F}$;*

and operates as follows:

- *User $l \in \mathcal{L}$ forms M_l and sends it to the fusion center over the public channel;*
- *The fusion center forms an estimate $\widehat{F}^n \triangleq d(M_{\mathcal{L}})$ of F^n.*

Definition 2. *A tuple $((R_l)_{l\in\mathcal{L}}, \Delta, (\Delta_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}})$ is achievable if there exists a sequence of $((2^{nR_l})_{l\in\mathcal{L}}, n)$ computation schemes such that for any $\mathcal{A} \in \mathbb{A}$*

$$\lim_{n\to\infty} \mathbb{P}[\widehat{F}^n \neq F^n] = 0, \tag{1}$$

$$\lim_{n\to\infty} \frac{1}{n} I(X_{\mathcal{L}}^n; M_{\mathcal{L}}|F^n) \leqslant \Delta, \tag{2}$$

$$\lim_{n\to\infty} \frac{1}{n} I(X_{\mathcal{A}^c}^n; M_{\mathcal{L}}|X_{\mathcal{A}}^n) \leqslant \Delta_{\mathcal{A}}, . \tag{3}$$

The set of all achievable tuples $((R_l)_{l\in\mathcal{L}}, \Delta, (\Delta_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}})$ is denoted by $\mathcal{C}(\mathbb{A})$.

(1) means that the fusion center obtains F^n with a small probability of error. (2) bounds the difference between $H(X_{\mathcal{L}}^n|F^n)$ and $H(X_{\mathcal{L}}^n|M_{\mathcal{L}}F^n)$, i.e., quantifies the leakage of the inputs $X_{\mathcal{L}}^n$ at the fusion center through the public communication $M_{\mathcal{L}}$, when accounting for the fact that the fusion center is supposed to learn F^n. Similarly, for $\mathcal{A} \in \mathbb{A}$, (3) bounds the difference between $H(X_{\mathcal{A}^c}^n|X_{\mathcal{A}}^n)$ and $H(X_{\mathcal{A}^c}^n|M_{\mathcal{L}}X_{\mathcal{A}}^n)$, i.e., quantifies the leakage of the inputs $X_{\mathcal{A}^c}^n$ at the set of colluding users $\mathcal{A}$ through the public communication $M_{\mathcal{L}}$, when accounting for the fact that the set of colluding users $\mathcal{A}$ has access to $X_{\mathcal{A}}^n$.

Example 1. *Suppose $\mathbb{A} = \{\{l\} : l \in \mathcal{L}\}$. Then, the users do not collude but each user is curious about the inputs of all the other users.*

Example 2. *Suppose $\mathbb{A} = \emptyset$. Then, the users are not interested in learning the inputs of the other users.*

Example 3. *Let $\mathcal{E}$ and $\mathcal{O}$ be the sets of even and odd indices in $\mathcal{L}$, respectively. Suppose $\mathbb{A} = \{\mathcal{E}, \mathcal{O}\}$. Then, the users with odd (respectively even) indices are interested in colluding to learn the inputs of the users with even (respectively odd) indices.*

III. Main Results

Theorem 1 (Converse)**.** *Let $\mathcal{P}^{\mathcal{O}}$ be the set of probability distributions $p_{U_{\mathcal{L}}X_{\mathcal{L}}}$ over $\mathcal{U}_{\mathcal{L}} \times \mathcal{X}_{\mathcal{L}}$ such that $U_{\mathcal{S}} - X_{\mathcal{S}} - X_{\mathcal{L}}, \forall \mathcal{S} \subseteq \mathcal{L}$, and $H(F|U_{\mathcal{L}}) = 0$. Next, define*

$$\mathcal{O}(\mathbb{A}) \triangleq \bigcup_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}\in\mathcal{P}^{\mathcal{O}}} \mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}}),$$

with $\mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}})$

$$\triangleq \{((R_l)_{l\in\mathcal{L}}, \Delta, (\Delta_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}}) : \forall \mathcal{S} \subseteq \mathcal{L}, \forall \mathcal{A} \in \mathbb{A},$$
$$R_{\mathcal{S}} \geqslant I(U_{\mathcal{S}}; X_{\mathcal{S}}|U_{\mathcal{S}^c}) - I(U_{\mathcal{S}}; U_{\mathcal{S}^c}|X_{\mathcal{S}}),$$
$$\Delta \geqslant I(U_{\mathcal{L}}; X_{\mathcal{L}}|F),$$
$$\Delta_{\mathcal{A}} \geqslant I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}|X_{\mathcal{A}})\}, \tag{4}$$

where for $\mathcal{S} \subseteq \mathcal{L}$, $R_{\mathcal{S}} \triangleq \sum_{l\in\mathcal{S}} R_l$, $X_{\mathcal{S}} = (X_l)_{l\in\mathcal{S}}$, and $U_{\mathcal{S}} = (U_l)_{l\in\mathcal{S}}$. Then, $\mathcal{C}(\mathbb{A}) \subseteq \mathcal{O}(\mathbb{A})$.

Proof. See Section V. ∎

Theorem 2 (Achievability)**.** *Let $\mathcal{P}^{\mathcal{I}}$ be the set of probability distributions $p_{U_{\mathcal{L}}X_{\mathcal{L}}}$ over $\mathcal{U}_{\mathcal{L}} \times \mathcal{X}_{\mathcal{L}}$ such that $p_{U_{\mathcal{L}}X_{\mathcal{L}}} = p_{X_{\mathcal{L}}} \prod_{l\in\mathcal{L}} p_{U_l|X_l}$ and $H(F|U_{\mathcal{L}}) = 0$. Next, define*

$$\mathcal{I}(\mathbb{A}) \triangleq \bigcup_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}\in\mathcal{P}^{\mathcal{I}}} \mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}}),$$

where $\mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}})$ is defined in (4)*. Then, $\mathcal{C}(\mathbb{A}) \supseteq \mathcal{I}(\mathbb{A})$.*

Proof. See Section VI. ∎

Note that the condition $p_{U_{\mathcal{L}}X_{\mathcal{L}}} = p_{X_{\mathcal{L}}} \prod_{l\in\mathcal{L}} p_{U_l|X_l}$ in Theorem 2 is more restrictive than the condition $U_{\mathcal{S}} - X_{\mathcal{S}} - X_{\mathcal{L}}, \forall \mathcal{S} \subseteq \mathcal{L}$ in Theorem 1. There is thus a gap between the achievability in Theorem 1 and the converse in Theorem 2. However, as shown in Theorem 3, in the case of independent inputs at the users, we tighten the converse to obtain the capacity region and show the optimality of the coding strategy in the proof of Theorem 2.

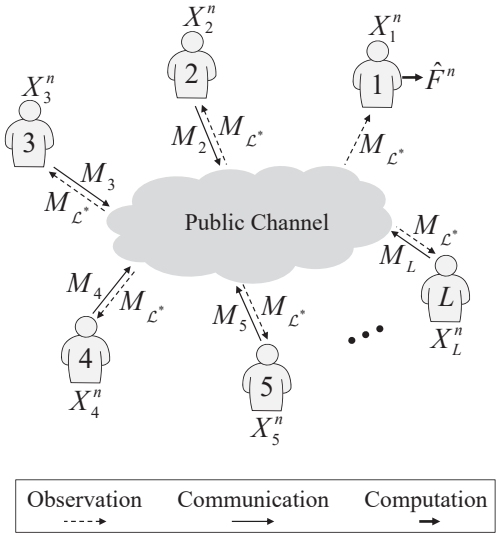

Fig. 2. Function computation over a public and noiseless broadcast channel with $l_0 = 1$. $M_{\mathcal{L}^*} \triangleq (M_l)_{l\in\mathcal{L}^*}$ is the overall public communication, with $\mathcal{L}^* \triangleq \mathcal{L}\backslash\{1\}$, and $\hat{F}^n$ is an estimate of $F^n \triangleq (f(X_{\mathcal{L},i}))_{i\in[\![1,n]\!]}$.

Theorem 3 (Capacity region for independent inputs)**.** *Assume that $p_{X_\mathcal{L}} = \prod_{l\in\mathcal{L}} p_{X_l}$. Let $\mathcal{P}$ be the set of probability distributions $p_{U_\mathcal{L}X_\mathcal{L}Q} = p_Q p_{X_\mathcal{L}} \prod_{l\in\mathcal{L}} p_{U_l|X_lQ}$ over $\mathcal{U}_\mathcal{L}\times\mathcal{X}_\mathcal{L}\times\mathcal{Q}$ such that $H(F|U_\mathcal{L}Q) = 0$, $|\mathcal{U}_l| \leqslant |\mathcal{X}_l|, \forall l \in \mathcal{L}$, and $|\mathcal{Q}| \leqslant L+|\mathbb{A}|+2$. Then, the capacity region is given by*

$$\mathcal{C}(\mathbb{A}) = \bigcup_{p_{U_\mathcal{L}X_\mathcal{L}Q}\in\mathcal{P}} \mathcal{T}(\mathbb{A}, p_{U_\mathcal{L}X_\mathcal{L}Q}),$$

with $\mathcal{T}(\mathbb{A}, p_{U_\mathcal{L}X_\mathcal{L}Q})$

$$\triangleq \{((R_l)_{l\in\mathcal{L}}, \Delta, (\Delta_\mathcal{A})_{\mathcal{A}\in\mathbb{A}}) : \forall l \in \mathcal{L}, \forall \mathcal{A} \in \mathbb{A},$$
$$R_l \geqslant I(U_l; X_l|Q),$$
$$\Delta \geqslant I(U_\mathcal{L}; X_\mathcal{L}|FQ),$$
$$\Delta_\mathcal{A} \geqslant I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}|Q)\}.$$

IV. Variant of the Model of Section II

Consider the same notation as in Section II. Fix $l_0 \in \mathcal{L}$ and define $\mathcal{L}^* \triangleq \mathcal{L}\backslash\{l_0\}$. For $\mathcal{A} \in \mathbb{A}$, define $\mathcal{A}^* \triangleq \mathcal{A}\backslash\{l_0\}$ and $\mathcal{A}^{c*} \triangleq \mathcal{A}^c\backslash\{l_0\}$. We consider the following variant of the setting of Section II as formalized in Definitions, 3, 4, and depicted in Figure 2. In this variant, there is no fusion center and a designated user (User l_0) needs to compute a function of all the users' private data including its own. Note that the model of Section II is not a special case of the model described in this section because the condition (2) is not necessarily present in this section.

Definition 3. *A $((2^{nR_l})_{l\in\mathcal{L}^*}, n)$ computation scheme consists of*

- *$L-1$ messages sets $\mathcal{M}_l \triangleq [\![1, 2^{nR_l}]\!]$, $l \in \mathcal{L}^*$;*
- *$L-1$ encoding functions $e_l : \mathcal{X}_l^n \to \mathcal{M}_l$, $l \in \mathcal{L}^*$;*
- *One decoding function $d : \mathcal{M}_{\mathcal{L}^*} \times \mathcal{X}_{l_0}^n \to \mathcal{F}$;*

and operates as follows:

- *User $l \in \mathcal{L}^*$ forms M_l and sends it over the public channel;*
- *User l_0 forms an estimate $\widehat{F}^n \triangleq d(M_{\mathcal{L}^*}, X_{l_0}^n)$ of F^n.*

Definition 4. *A tuple $((R_l)_{l\in\mathcal{L}^*}, (\Delta_\mathcal{A})_{\mathcal{A}\in\mathbb{A}})$ is achievable if there exists a sequence of $((2^{nR_l})_{l\in\mathcal{L}^*}, n)$ computation schemes such that for any $\mathcal{A} \in \mathbb{A}$*

$$\lim_{n\to\infty} \mathbb{P}[\widehat{F}^n \neq F^n] = 0, \tag{5}$$

$$\lim_{n\to\infty} \frac{1}{n} I(X_{\mathcal{A}^c}^n; M_{\mathcal{L}^*}|\bar{F}^n X_\mathcal{A}^n) \leqslant \Delta_\mathcal{A},, \tag{6}$$

where $\bar{F}^n \triangleq \begin{cases} F^n & \text{if } l_0 \in \mathcal{A} \\ \emptyset & \text{if } l_0 \notin \mathcal{A} \end{cases}$. The set of all achievable tuples $((R_l)_{l\in\mathcal{L}}, (\Delta_\mathcal{A})_{\mathcal{A}\in\mathbb{A}})$ is denoted by $\mathcal{C}(\mathbb{A}, l_0)$.

(5) means that User l_0 can reconstruct F^n. For $\mathcal{A} \in \mathbb{A}$, (6) bounds the difference between $H(X_{\mathcal{A}^c}^n|\bar{F}^n X_\mathcal{A}^n)$ and $H(X_{\mathcal{A}^c}^n|\bar{F}^n M_{\mathcal{L}^*} X_\mathcal{A}^n)$, i.e., quantifies the leakage of the inputs $X_{\mathcal{A}^c}^n$ at the set of colluding users $\mathcal{A}$ through the public communication $M_{\mathcal{L}^*}$, when accounting for the fact that the set of colluding users $\mathcal{A}$ has access to $(X_\mathcal{A}^n, \bar{F}^n)$.

Theorem 4 (Capacity region for independent inputs)**.** *Assume that $p_{X_\mathcal{L}} = \prod_{l\in\mathcal{L}} p_{X_l}$. Let $\mathcal{P}$ be the set of probability distributions $p_{U_{\mathcal{L}^*}X_\mathcal{L}Q} = p_Q p_{X_\mathcal{L}} \prod_{l\in\mathcal{L}^*} p_{U_l|X_lQ}$ over $\mathcal{U}_{\mathcal{L}^*}\times\mathcal{X}_\mathcal{L}\times\mathcal{Q}$ such that $H(F|U_{\mathcal{L}^*}X_{l_0}Q) = 0$, $|\mathcal{U}_l| \leqslant |\mathcal{X}_l|, \forall l \in \mathcal{L}^*$, and $|\mathcal{Q}| \leqslant L + |\mathbb{A}|$. Then, the capacity region is given by*

$$\mathcal{C}(\mathbb{A}, l_0) = \bigcup_{p_{U_{\mathcal{L}^*}X_\mathcal{L}Q}\in\mathcal{P}} \mathcal{T}(\mathbb{A}, p_{U_{\mathcal{L}^*}X_\mathcal{L}Q}), \text{ where}$$

$$\mathcal{T}(\mathbb{A}, p_{U_{\mathcal{L}^*}X_\mathcal{L}Q})$$
$$\triangleq \{((R_l)_{l\in\mathcal{L}^*}, (\Delta_\mathcal{A})_{\mathcal{A}\in\mathbb{A}}) : \forall l \in \mathcal{L}^*,$$
$$R_l \geqslant I(U_l; X_l|Q),$$
$$\Delta_\mathcal{A} \geqslant I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}|FQX_\mathcal{A}), \forall \mathcal{A}\in\mathbb{A}, \text{s.t. } \mathcal{A}\ni l_0$$
$$\Delta_\mathcal{A} \geqslant I(X_{\mathcal{A}^{c*}}; U_{\mathcal{A}^{c*}}|Q), \forall \mathcal{A}\in\mathbb{A}, \text{s.t. } \mathcal{A}\not\ni l_0\}.$$

Example 4. *Assume $L = 2$, $l_0 = 2$, $p_{X_1X_2} = p_{X_1}p_{X_2}$, and $\mathbb{A} = \{\{2\}\}$. Let $\mathcal{P}$ be as in Theorem 4. Then,*

$$\mathcal{C}(\mathbb{A}, l_0) = \{(R_1, \Delta_{\{2\}}) : R_1 \geqslant I(U_1^*; X_1),$$
$$\Delta_{\{2\}} \geqslant I(U_1^*; X_1) - I(F; X_1|X_2)\},$$

where $I(U_1^*; X_1) \triangleq \min_{p_{U_1X_1}\in\mathcal{P}} I(U_1; X_1)$.

As we can see from this example, there is a linear relationship between communication rate R_1 and leakage $\Delta_{\{2\}}$ as $I(F; X_1|X_2)$ is a constant term.

V. Proof of Theorem 1

For $l \in \mathcal{L}$ and $j \in [\![1, n]\!]$, we write $X_l^j \triangleq (X_{l,i})_{i\in[\![1,j]\!]}$. Then, for $\mathcal{S} \subseteq \mathcal{L}$, we have

$$R_\mathcal{S} \overset{(a)}{\geqslant} \frac{1}{n}\sum_{l\in\mathcal{S}} H(M_l)$$
$$\geqslant \frac{1}{n} I(M_\mathcal{S}; X_\mathcal{S}^n) \tag{7}$$
$$\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^n I(M_\mathcal{S}; X_{\mathcal{S},i}|X_\mathcal{S}^{i-1})$$
$$\overset{(c)}{=} \frac{1}{n}\sum_{i=1}^n I(M_\mathcal{S} X_\mathcal{S}^{i-1}; X_{\mathcal{S},i}) \tag{8}$$

$$\begin{aligned}
&\overset{(d)}{=} \frac{1}{n}\sum_{i=1}^{n} I(M_{\mathcal{S}}X_{\mathcal{L}}^{i-1}; X_{\mathcal{S},i}) \\
&\overset{(e)}{=} \frac{1}{n}\sum_{i=1}^{n} I(U_{\mathcal{S},i}; X_{\mathcal{S},i}) \\
&\overset{(f)}{=} I(U_{\mathcal{S}}; X_{\mathcal{S}}) \\
&= I(U_{\mathcal{S}}; X_{\mathcal{S}}U_{\mathcal{S}^c}) - I(U_{\mathcal{S}}; U_{\mathcal{S}^c}|X_{\mathcal{S}}) \\
&\geqslant I(U_{\mathcal{S}}; X_{\mathcal{S}}|U_{\mathcal{S}^c}) - I(U_{\mathcal{S}}; U_{\mathcal{S}^c}|X_{\mathcal{S}}),
\end{aligned} \tag{9}$$

where (a) holds by Definition 1, (b) holds by the chain rule with the notation $X_{\mathcal{S},i} \triangleq (X_{l,i})_{l\in\mathcal{S}}$ and $X_{\mathcal{S}}^{i-1} \triangleq (X_l^{i-1})_{l\in\mathcal{S}}$, (c) holds by independence between $X_{\mathcal{S}}^{i-1}$ and $X_{\mathcal{S},i}$, (d) holds because $I(X_{\mathcal{S}^c}^{i-1}; X_{\mathcal{S},i}|M_{\mathcal{S}}X_{\mathcal{S}}^{i-1}) \leqslant I(X_{\mathcal{S}^c}^{i-1}; X_{\mathcal{S},i}M_{\mathcal{S}}|X_{\mathcal{S}}^{i-1}) \leqslant I(X_{\mathcal{S}^c}^{i-1}; X_{\mathcal{S}}^n|X_{\mathcal{S}}^{i-1}) = 0$, (e) holds with $U_{l,i} \triangleq (M_l, X_{\mathcal{L}}^{i-1})$ and the notation $U_{\mathcal{S},i} \triangleq (U_{l,i})_{l\in\mathcal{S}}$, (f) holds with $U_l \triangleq (I, U_{l,I})$ where I is uniformly distributed over $[\![1,n]\!]$ and independent of all other random variables. Next, using Fano's inequality, the chain rule, the data processing inequality, and the definition of $U_{l,i}$, $l \in \mathcal{L}$, $i \in [\![1,n]\!]$ one can show

$$o(n) = nH(F|U_{\mathcal{L}}). \tag{10}$$

Next, by (2) we have

$$\begin{aligned}
\Delta &\geqslant \frac{1}{n} I(X_{\mathcal{L}}^n; M_{\mathcal{L}}|F^n) \\
&= \frac{1}{n} I(X_{\mathcal{L}}^n; M_{\mathcal{L}}) + \frac{1}{n} I(X_{\mathcal{L}}^n; F^n|M_{\mathcal{L}}) - I(X_{\mathcal{L}}; F) \\
&\overset{(a)}{=} \frac{1}{n} I(X_{\mathcal{L}}^n; M_{\mathcal{L}}) - I(X_{\mathcal{L}}; F) + o(1) \\
&\overset{(b)}{=} I(U_{\mathcal{L}}; X_{\mathcal{L}}) - I(X_{\mathcal{L}}; F) + o(1) \\
&= I(U_{\mathcal{L}}; X_{\mathcal{L}}|F) + I(U_{\mathcal{L}}; F) - I(X_{\mathcal{L}}; F) + o(1) \\
&\overset{(c)}{=} I(U_{\mathcal{L}}; X_{\mathcal{L}}|F) + o(1),
\end{aligned} \tag{11}$$

where (a) holds by Fano's inequality and (1), (b) holds by the steps between (7) and (9) by choosing $\mathcal{S} = \mathcal{L}$, (c) holds because $I(U_{\mathcal{L}}; F) - I(X_{\mathcal{L}}; F) = H(F|X_{\mathcal{L}}) - H(F|U_{\mathcal{L}}) = -H(F|U_{\mathcal{L}}) = o(1)$ by (10).

Finally, by (3) we have for $\mathcal{A} \in \mathbb{A}$

$$\begin{aligned}
\Delta_{\mathcal{A}} &\geqslant \frac{1}{n} I(X_{\mathcal{A}^c}^n; M_{\mathcal{L}}|X_{\mathcal{A}}^n) \\
&= \frac{1}{n} I(X_{\mathcal{A}^c}^n; M_{\mathcal{A}^c}|X_{\mathcal{A}}^n) \\
&\overset{(a)}{=} \frac{1}{n} I(X_{\mathcal{A}^c}^n; M_{\mathcal{A}^c}) - \frac{1}{n} I(X_{\mathcal{A}}^n; M_{\mathcal{A}^c}) \\
&\overset{(b)}{=} I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - \frac{1}{n} I(X_{\mathcal{A}}^n; M_{\mathcal{A}^c}) \\
&= I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - \frac{1}{n}\sum_{i=1}^{n} I(X_{\mathcal{A},i}; M_{\mathcal{A}^c}|X_{\mathcal{A}}^{i-1}) \\
&\overset{(c)}{=} I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - \frac{1}{n}\sum_{i=1}^{n} I(X_{\mathcal{A},i}; M_{\mathcal{A}^c}X_{\mathcal{A}}^{i-1}) \\
&\geqslant I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - \frac{1}{n}\sum_{i=1}^{n} I(X_{\mathcal{A},i}; M_{\mathcal{A}^c}X_{\mathcal{L}}^{i-1}) \\
&= I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - \frac{1}{n}\sum_{i=1}^{n} I(X_{\mathcal{A},i}; U_{\mathcal{A}^c,i}) \\
&= I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}) - I(X_{\mathcal{A}}; U_{\mathcal{A}^c}) \\
&\overset{(d)}{=} I(X_{\mathcal{A}^c}; U_{\mathcal{A}^c}|X_{\mathcal{A}}),
\end{aligned} \tag{12}$$

where (a) holds because $M_{\mathcal{A}^c} - X_{\mathcal{A}^c}^n - X_{\mathcal{A}}^n$, (b) holds by the steps between (7) and (9) by choosing $\mathcal{S} = \mathcal{A}^c$, (c) holds by independence between $X_{\mathcal{A}}^{i-1}$ and $X_{\mathcal{A},i}$, (d) holds because $U_{\mathcal{A}^c} - X_{\mathcal{A}^c} - X_{\mathcal{A}}$ since for any $\mathcal{S} \subseteq \mathcal{L}$, $U_{\mathcal{S}} - X_{\mathcal{S}} - X_{\mathcal{L}}$ forms a Markov chain because for any $i \in [\![1,n]\!]$, we have $I(U_{\mathcal{S},i}; X_{\mathcal{L},i}|X_{\mathcal{S},i}) = I(M_{\mathcal{S}}X_{\mathcal{L}}^{i-1}; X_{\mathcal{L},i}|X_{\mathcal{S},i}) \leqslant I(X_{\mathcal{S}}^n X_{\mathcal{L}}^{i-1}; X_{\mathcal{L},i}|X_{\mathcal{S},i}) = 0$, which implies $0 = I(U_{\mathcal{S},I}; X_{\mathcal{L},I}|X_{\mathcal{S},I}I) = I(U_{\mathcal{S},I}I; X_{\mathcal{L},I}|X_{\mathcal{S},I}) = I(U_{\mathcal{S}}; X_{\mathcal{L}}|X_{\mathcal{S}})$.

VI. Proof of Theorem 2

A. Reduction of the achievability of $\mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}})$

Lemma 1. *Fix $p_{U_{\mathcal{L}}X_{\mathcal{L}}} = p_{X_{\mathcal{L}}}\prod_{l\in\mathcal{L}} p_{U_l|X_l}$. Then, the set function $g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}$ is normalized, non-decreasing, and supermodular, where $g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}} : 2^{\mathcal{L}} \to \mathbb{R}, \mathcal{S} \mapsto I(U_{\mathcal{S}}; X_{\mathcal{L}}|U_{\mathcal{S}^c})$.*

Lemma 2. *Fix $p_{U_{\mathcal{L}}X_{\mathcal{L}}} = p_{X_{\mathcal{L}}}\prod_{l\in\mathcal{L}} p_{U_l|X_l}$. Then,*

$$\mathcal{P}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}) \triangleq \left\{(R_l)_{l\in\mathcal{L}} \in \mathbb{R}_+^L : R_{\mathcal{S}} \geqslant g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}(\mathcal{S}), \forall \mathcal{S} \subseteq \mathcal{L}\right\}$$

associated with the function $g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}$ defined in Lemma 1, is a contrapolymatroid, and any point in $\mathcal{P}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}})$ is dominated by a point in the dominant face $\mathcal{D}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}})$, where

$$\mathcal{D}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}) \triangleq \left\{(R_l)_{l\in\mathcal{L}} \in \mathcal{P}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}) : R_{\mathcal{L}} = g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}(\mathcal{L})\right\}.$$

Additionally, by denoting the symmetric group on $\mathcal{L}$ by Sym(L), the dominant face has the following characterization:

$$\mathcal{D}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}) = \mathit{Conv}\left(\left\{(C_{\pi(l)})_{l\in\mathcal{L}} : \pi \in \mathit{Sym}(L)\right\}\right), \tag{13}$$

with

$$C_{\pi(l)} \triangleq I(U_{\pi(l)}; X_{\pi(l)}|U_{\pi(1:l-1)}), \forall \pi \in \mathit{Sym}(L), \forall l \in \mathcal{L},$$

where we used the notation $\pi(i:j) \triangleq \{\pi(k) : k \in [\![i,j]\!]\})$ for $i, j \in \mathcal{L}$.

Lemma 3. *Fix $p_{U_{\mathcal{L}}X_{\mathcal{L}}} = p_{X_{\mathcal{L}}}\prod_{l\in\mathcal{L}} p_{U_l|X_l}$ and define*

$$\bar{g}_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}} : 2^{\mathcal{L}} \to \mathbb{R}, \mathcal{S} \mapsto I(U_{\mathcal{S}}; X_{\mathcal{S}}|U_{\mathcal{S}^c}) - I(U_{\mathcal{S}}; U_{\mathcal{S}^c}|X_{\mathcal{S}}).$$

Then, $\bar{g}_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}} = g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}$.

By Lemma 3, $\mathcal{P}(\bar{g}_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}}) = \mathcal{P}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}})$. Then, by Lemma 2, to prove the achievability of $\mathcal{P}(g_{p_{U_{\mathcal{L}}X_{\mathcal{L}}}})$, it is sufficient to prove the achievability of the corner point $(I(U_l; X_l|U_{1:l-1}))_{l\in\mathcal{L}}$, as the other corners points can be achieved similarly by relabelling the users and any point of the dominant face can be achieved by time-sharing between the corner points $\left\{(C_{\pi(l)})_{l\in\mathcal{L}} : \pi \in \mathrm{Sym}(L)\right\}$. Hence, since the constraints in (2) and (3) are preserved under time sharing, the achievability of $((I(U_l; X_l|U_{1:l-1}))_{l\in\mathcal{L}}, \Delta, (\Delta_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}})$, with the notation $(U_{1:l-1}) \triangleq (U_{[\![1,l-1]\!]})$, implies the achievability of $\mathcal{R}(\mathbb{A}, p_{U_{\mathcal{L}}X_{\mathcal{L}}})$.

B. Achievability of $((I(U_l;X_l|U_{1:l-1}))_{l\in\mathcal{L}},\Delta,(\Delta_{\mathcal{A}})_{\mathcal{A}\in\mathbb{A}})$

For $n\in\mathbb{N}$, $\epsilon>0$, and a probability mass function p_{XY} defined over $\mathcal{X}\times\mathcal{Y}$, denote the set of ϵ-typical n-sequences, e.g., [3], [13], by $\mathcal{T}_\epsilon^n(p_{XY})$, and define for $y^n\in\mathcal{Y}^n$, the set of conditionally ϵ-typical n-sequences by $\mathcal{T}_\epsilon^n(p_{XY}|y^n)$.

Codebook construction. For $l\in\mathcal{L}$, consider $R_l>0$ and $\widetilde{R}_l>0$ to be defined later in the coding scheme analysis. Fix $p_{U_{\mathcal{L}}X_{\mathcal{L}}}=p_{X_{\mathcal{L}}}\prod_{l\in\mathcal{L}}p_{U_l|X_l}$ such that $H(F|U_{\mathcal{L}})=0$, and construct a codebook $\mathcal{C}$ as follows. For each $l\in\mathcal{L}$, generate $2^{n\widetilde{R}_l}$ independent sequences $u_l^n(\omega_l)$, indexed by $\omega_l\in[\![1,2^{n\widetilde{R}_l}]\!]$, according to $\prod_{i=1}^n p_{U_l}$, and partition the $2^{n\widetilde{R}_l}$ indices into 2^{nR_l} equal-size bins indexed by $m_l\in[\![1,2^{nR_l}]\!]$. Fix $(\epsilon_l)_{l\in[\![0,L]\!]}$ a strictly increasing sequence in $\mathbb{R}_{>0}^{L+1}$.

Encoding at User $l\in\mathcal{L}$: Find $\omega_l\in[\![1,2^{n\widetilde{R}_l}]\!]$ such that $(x_l^n,u_l^n(\omega_l))\in\mathcal{T}_{\epsilon_0}^n(p_{X_lU_l})$ and send the corresponding bin number m_l over the public channel. If multiple sequences are found, then choose one at random, and if none are found, then choose m_l uniformly at random over $[\![1,2^{n\widetilde{R}_l}]\!]$.

Decoding: For l from 1 to L, find the unique $\hat{\omega}_l$ with bin number m_l such that $u_{1:l}^n(\hat{\omega}_{1:l})\in\mathcal{T}_{\epsilon_L}^n(p_{U_{1:l}})$ – if no such index exists, then return an error. Note that since $H(F|U_{\mathcal{L}})=0$, there exists a deterministic function $\tilde{F}$ such that $\tilde{F}(u_{\mathcal{L}})=F(x_{\mathcal{L}})$, for all $(u_{\mathcal{L}},x_{\mathcal{L}})$ such that $p(u_{\mathcal{L}},x_{\mathcal{L}})>0$. Then, the decoder computes $\widehat{F}^n\triangleq\tilde{F}(u_{\mathcal{L}}^n(\hat{\omega}_{\mathcal{L}}))$.

C. Coding scheme analysis

Error probability and rates: First, one can show that

$$\mathbb{P}[\{(U_{1:L}^n(\Omega_{1:L}),X_{\mathcal{L}}^n)\notin\mathcal{T}_{\epsilon_L}^n(p_{U_{1:L}X_{\mathcal{L}}})\}]\xrightarrow{n\to\infty}0 \tag{14}$$

by choosing

$$\widetilde{R}_l\triangleq I(U_l;X_l)+\delta(\epsilon_{l-1}),\forall l\in\mathcal{L}. \tag{15}$$

Then, by (14) and by choosing

$$R_l>\widetilde{R}_l-I(U_l;U_{1:l-1})+\delta_l(\epsilon_L),\forall l\in\mathcal{L} \tag{16}$$

for some $\delta_l(\epsilon_L)$ such that $\lim_{\epsilon_L\to0}\delta_l(\epsilon_L)=0$, one can show that $\mathbb{P}[\widehat{F}^n\neq F^n]\xrightarrow{n\to\infty}0$, and by (15), (16). Finally, by the Markov chain $U_l-X_l-U_{1:l-1}$, we have

$$R_l>I(U_l;X_l|U_{1:l-1})+\delta(\epsilon_{l-1})+\delta_l(\epsilon_L). \tag{17}$$

Leakage at the fusion center: We have

$$\begin{aligned}
&\frac{1}{n}I(X_{\mathcal{L}}^n;M_{\mathcal{L}}|F^n\mathcal{C})\\
&\overset{(a)}{\leqslant}\frac{1}{n}\sum_{l\in\mathcal{L}}H(M_l)+o(1)-I(X_{\mathcal{L}};F)\\
&\overset{(b)}{\leqslant}\sum_{l\in\mathcal{L}}I(U_l;X_l|U_{1:l-1})+o(1)-I(X_{\mathcal{L}};F)\\
&\overset{(c)}{=}\sum_{l\in\mathcal{L}}I(U_l;X_{\mathcal{L}}|U_{1:l-1})+o(1)-I(X_{\mathcal{L}};F)\\
&=I(U_{\mathcal{L}};X_{\mathcal{L}})+o(1)-I(X_{\mathcal{L}};F)\\
&\overset{(d)}{=}I(U_{\mathcal{L}};X_{\mathcal{L}}|F)+o(1),
\end{aligned}$$

where (a) can be obtained with Fano's inequality, (b) holds by (17), (c) holds because $U_l-(X_l,U_{1:l-1})-X_{\mathcal{L}\setminus\{l\}}$, (d) holds because $H(X_{\mathcal{L}}|U_{\mathcal{L}})=H(X_{\mathcal{L}}F|U_{\mathcal{L}})=H(X_{\mathcal{L}}|FU_{\mathcal{L}})+H(F|U_{\mathcal{L}})=H(X_{\mathcal{L}}|FU_{\mathcal{L}})$.

Leakage at colluding users in $\mathcal{A}\in\mathbb{A}$: Define $\Upsilon\triangleq\mathbb{1}\{(U_{\mathcal{L}}^n(\Omega_{\mathcal{L}}),X_{\mathcal{L}}^n)\in\mathcal{T}_{\epsilon_L}^n(p_{U_{\mathcal{L}}X_{\mathcal{L}}})\}$. We have

$$\begin{aligned}
&\frac{1}{n}I(X_{\mathcal{A}^c}^n;M_{\mathcal{L}}|X_{\mathcal{A}}^n\mathcal{C})\\
&\leqslant\frac{1}{n}I(X_{\mathcal{A}^c}^n;M_{\mathcal{L}}U_{\mathcal{L}}^n(\Omega_{\mathcal{L}})|X_{\mathcal{A}}^n\mathcal{C})\\
&=\frac{1}{n}I(X_{\mathcal{A}^c}^n;U_{\mathcal{L}}^n(\Omega_{\mathcal{L}})|X_{\mathcal{A}}^n\mathcal{C})\\
&=H(X_{\mathcal{A}^c}|X_{\mathcal{A}})-H(X_{\mathcal{A}^c}^n|U_{\mathcal{L}}^n(\Omega_{\mathcal{L}})X_{\mathcal{A}}^n\mathcal{C})\\
&\overset{(b)}{\leqslant}H(X_{\mathcal{A}^c}|X_{\mathcal{A}})-\mathbb{P}[\Upsilon=1]H(X_{\mathcal{A}^c}^n|U_{\mathcal{L}}^n(\Omega_{\mathcal{L}})X_{\mathcal{A}}^n\mathcal{C},\Upsilon=1)\\
&\xrightarrow{n\to\infty,\epsilon_L\to0}-H(U_{\mathcal{A}^c}|X_{\mathcal{A}^c})+H(U_{\mathcal{A}^c}|X_{\mathcal{A}})\\
&=I(U_{\mathcal{A}^c};X_{\mathcal{A}^c}|X_{\mathcal{A}}),
\end{aligned}$$

where (a) holds because conditioning reduces entropy, and the limit holds by (14) and because for $(u_{\mathcal{L}}^n,x_{\mathcal{L}}^n)\in\mathcal{T}_{\epsilon_L}^n(p_{U_{\mathcal{L}}X_{\mathcal{L}}})$

$$\begin{aligned}
p(x_{\mathcal{A}^c}^n|u_{\mathcal{L}}^n,x_{\mathcal{A}}^n)&=\frac{p(x_{\mathcal{L}}^n)p(u_{\mathcal{L}}^n|x_{\mathcal{L}}^n)}{p(x_{\mathcal{A}}^n)p(u_{\mathcal{A}}^n|x_{\mathcal{A}}^n)p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}}^nu_{\mathcal{A}}^n)}\\
&\overset{(b)}{=}\frac{p(x_{\mathcal{A}^c}^n|x_{\mathcal{A}}^n)\prod_{l\in\mathcal{A}^c}p(u_l^n|x_l^n)}{p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}}^nu_{\mathcal{A}}^n)}\\
&\overset{(c)}{=}\frac{p(x_{\mathcal{A}^c}^n|x_{\mathcal{A}}^n)p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}^c}^n)}{p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}}^n)}\\
&\overset{(d)}{\leqslant}2^{-n(H(X_{\mathcal{A}^c}|X_{\mathcal{A}})+H(U_{\mathcal{A}^c}|X_{\mathcal{A}^c})-2\delta(\epsilon_L))}\\
&\quad\times(1-\epsilon_L)^{-1}2^{n(H(U_{\mathcal{A}^c}|X_{\mathcal{A}})+\delta(\epsilon_L))},
\end{aligned}$$

where (b) holds because for any $l\in\mathcal{L}$, $U_l^n(\Omega_l)-X_l^n-(X_{\mathcal{L}\setminus\{l\}}^n,U_{\mathcal{L}\setminus\{l\}}^n(\Omega_{\mathcal{L}\setminus\{l\}}))$, (c) holds because $U_{\mathcal{A}^c}^n(\Omega_{\mathcal{A}^c})-X_{\mathcal{A}}^n-U_{\mathcal{A}}^n(\Omega_{\mathcal{A}})$ forms a Markov chain, (d) holds for some $\delta(\epsilon_L)$ such that $\lim_{\epsilon_L\to0}\delta(\epsilon_L)=0$ because $p(x_{\mathcal{A}^c}^n|x_{\mathcal{A}}^n)\leqslant2^{-n(H(X_{\mathcal{A}^c}|X_{\mathcal{A}})-\delta(\epsilon_L))}$ from the properties of typical sequences since $x_{\mathcal{L}}^n\in\mathcal{T}_{\epsilon_L}^n(p_{X_{\mathcal{L}}})$, and $p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}}^n)\geqslant(1-\epsilon_L)2^{-n(H(U_{\mathcal{A}^c}|X_{\mathcal{A}})+\delta(\epsilon_L))}$ and $p(u_{\mathcal{A}^c}^n|x_{\mathcal{A}^c}^n)\leqslant2^{-n(H(U_{\mathcal{A}^c}|X_{\mathcal{A}^c})-\delta(\epsilon_L))}$, which is obtained using that $(u_{\mathcal{L}}^n,x_{\mathcal{L}}^n)\in\mathcal{T}_{\epsilon_L}^n(p_{U_{\mathcal{L}}X_{\mathcal{L}}})$ similar to [13, Lemma 12.3].

VII. Concluding Remarks

We considered a function computation setting among multiple users where only a public and noiseless broadcast channel is available to the users. We focused on studying optimal communication and information leakage rates on the private user data for two models. In the first one, a fusion center needs to compute a function of the private user data. In the second one, there is no fusion center and a specific user must compute a function of the private data of all the users, including theirs. For both settings, we derived a capacity region when the data of the users is independent. We derived inner and outer regions for the capacity region of the first setting when the data of the users is correlated. We note that such inner and outer regions can also be derived for the capacity region of the second setting and are not reported here.

REFERENCES

[1] R. A. Chou and J. Kliewer, "Function computation without secure links: Information and leakage rates," *arXiv preprint arXiv:2201.11891*, 2022.

[2] R. Cramer, I. Damgård, and J. Nielsen, *Secure Multiparty Computation*. Cambridge University Press, 2015.

[3] A. Orlitsky and J. Roche, "Coding for computing," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 903–917, 2001.

[4] M. Sefidgaran and A. Tchamkerten, "Distributed function computation over a rooted directed tree," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7135–7152, 2016.

[5] N. Ma and P. Ishwar, "Some results on distributed source coding for interactive function computation," *IEEE Transactions on Information Theory*, vol. 57, no. 9, pp. 6180–6195, 2011.

[6] N. Ma, P. Ishwar, and P. Gupta, "Interactive source coding for function computation in collocated networks," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4289–4305, 2012.

[7] N. Ma and P. Ishwar, "The infinite-message limit of two-terminal interactive source coding," *IEEE Transactions on Information Theory*, vol. 59, no. 7, pp. 4071–4094, 2013.

[8] D. Data, V. M. Prabhakaran, and M. M. Prabhakaran, "Communication and randomness lower bounds for secure computation," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3901–3929, 2016.

[9] E. J. Lee and E. Abbe, "Two Shannon-type problems on secure multiparty computations," in *52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2014, pp. 1287–1293.

[10] D. Data, G. R. Kurri, J. Ravi, and V. M. Prabhakaran, "Interactive secure function computation," *IEEE Transactions on Information Theory*, vol. 66, no. 9, pp. 5492–5521, 2020.

[11] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6337–6350, 2011.

[12] W. Tu and L. Lai, "On function computation with privacy and secrecy constraints," *IEEE Transactions on Information Theory*, vol. 65, no. 10, pp. 6716–6733, 2019.

[13] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.