On Function Computation With Privacy and Secrecy Constraints

Wenwen Tu and Lifeng Lai, *Member, IEEE*

***Abstract*— In this paper, the problem of function computation with privacy and secrecy constraints is considered. The considered model consists of three legitimate nodes (i.e., two transmitters, Alice and Bob, and a fusion center that acts as the receiver) that observe correlated sources and are connected by noiseless public channels, and an eavesdropper Eve who has full access to the public channels and also has its own source observations. The fusion center would like to compute a function of the distributed sources within a prefixed distortion level under a certain distortion metric. To facilitate the function computation, Alice and Bob will send messages to the fusion center. Different from the existing setups in function computation, we assume that there is a *privacy* constraint on the sources at Alice and Bob. In particular, Alice and Bob would like to enable the fusion center to compute the function, but at same time, they do not want the fusion center to learn too much information about the source observations. We introduce a quantity to precisely measure the privacy leakage to the fusion center. In addition to this privacy constraint, we also have a *secrecy* constraint to Eve and use equivocation of sources to measure this quantity. Under this model, we study the tradeoffs among message rates, private information leakage, equivocation, and distortion. We first consider a scenario that has only one transmitter, i.e., the source at Bob is empty, and fully single-letter characterize the corresponding regions. Then, we consider the more general case and provide both outer and inner bounds on the corresponding regions.**

***Index Terms*— Function computation, privacy constraint, public discussion, rate distortion, secrecy constraint.**

I. Introduction

RECENTLY, the problem of designing schemes to enable communication parties to compute functions of distributed sources has received significant attentions [3]–[19]. One straightforward scheme for function computation is to ask each information source to send enough information (for example, using schemes in distributed source coding [20]–[25]) so that the function computing parties can first recover all sources and then compute functions of interest using the recovered sources. However, as shown in many of the existing works, full source recovery is not necessary in many scenarios [13]–[18]. As the result, information sources can reduce their transmitted message rates while still enabling the function computing parties to compute functions of interest. This can significantly reduce the resource (in terms of energy, spectrum, etc.) requirements and hence is very appealing for resource-constrained applications such as IoT where the goal of communication is decision making (hence requires function computation) but not full source recovery [26]–[29].

In the basic function computation setup considered in [13], two terminals observe correlated sources and are allowed to exchange messages, while only one of them is required to compute a function of these distributed sources. Reference [13] investigates the minimum message rates so that the function can be computed with a negligibly small error probability. It characterizes the message rate region and further provides an efficient method, by introducing conditional characteristic graph, to characterize the optimal message rate for the case where only one terminal is allowed to send messages. This basic model is further extended to more complex scenarios in many interesting recent papers [14]–[18]. In particular, [14] studies the problem of two-terminal interactive distributed source coding for function computations at both terminals. In this model, these two terminals are allowed to exchange t (a finite nonnegative integer) coded messages, and each terminal needs to compute a function within a certain distortion level. Reference [14] provides a single-letter characterization on the corresponding message rate region. Properties of the limit of the sum-rate-distortion function (i.e., the minimal value of the sum of message rates) when t goes to infinity are further investigated in [16]. Furthermore, [17] studies the message rate region of function computation in a different setup. The model considered in [17] consists of three terminals, two of them (transmitters) are allowed to send messages to the third terminal who needs to compute a function, but there is no interaction between the two transmitters. This model is further discussed in [18] by allowing an additional one-way discussion between the two transmitters. Reference [19] further generalizes this model to a more sophisticated scenario that consists of more terminals over a rooted multi-level directed tree. In this scenario, each terminal is allowed to transmit messages to its parent terminal and the function is computed at the root. Reference [19] provides both outer and inner bounds on the message rate region, which recover capacity regions of many function computation setups.

Manuscript received June 16, 2017; revised March 15, 2019; accepted June 6, 2019. Date of publication June 13, 2019; date of current version September 13, 2019. W. Tu and L. Lai were supported by the National Science Foundation under Grant CCF-1665073, Grant ECCS-1660140, and Grant CNS-1824553. This paper was presented in part at the 2017 Asilomar Conference on Signals, Systems, and Computers [1] and in part at the 2018 IEEE International Workshop on Signal Processing Advances in Wireless Communications [2].

W. Tu is with Black Sesame Technologies Inc., Santa Clara, CA 95050 USA (e-mail: wwtu@ucdavis.edu).

L. Lai is with the Department of Electrical and Computer Engineering, University of California at Davis, Davis, CA 95616 USA (e-mail: lflai@ucdavis.edu).

Communicated by E. Tuncel, Associate Editor for Source Coding.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2019.2922634

In this paper, we consider privacy and secrecy issues arising in the function computation setup. In the considered model, two terminals, Alice and Bob, are connected to a fusion center, and they observe correlated source sequences X_1^n, X_2^n, Y^n respectively. The fusion center would like to compute a function of X_1^n, X_2^n, Y^n. To facilitate the function computation, Alice and Bob will send messages M_1 and M_2 respectively to the fusion center. Different from the setups in [13]–[16], we assume that there is a *privacy* constraint on the sources at Alice and Bob. In particular, these terminals would like to assist the fusion center to compute the function but at same time do not want the fusion center to learn too much information about their source observations. We use $\frac{1}{n}I(X_1^n, X_2^n; M_1, M_2|Y^n)$ as our privacy measure. As this quantity is the same as $\frac{1}{n}[H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n)]$, this quantity measures additional information about the sources (X_1^n, X_2^n) that the fusion center learns from the transmitted messages. We would like to minimize this privacy leakage subject to the constraint that the fusion center can still compute the function of interest. In addition to this privacy constraint, we also have a *secrecy* constraint. In particular, there is an additional terminal Eve who observes Z^n, which is correlated with the source sequences, and we use equivocation of sources to measure the secrecy leakage to Eve. We would like to maximize this equivocation so that Eve's uncertainty about the sources is maximized.

For the function to be computed, we consider both lossless and lossy cases. In the lossless case, the fusion center is required to compute the function with a diminishingly small error probability. In the lossy case, we allow the computed function to be within a certain distortion level measured by a given distortion metric. We would like to note that the lossless case in our model is not merely a special case of the lossy case when the distortion is zero. It will be clear in the sequel, the lossless case in our model has a more stringent constraint than just setting distortion as zero in the lossy case. Thus, it deserves an independent study. We study the relationship of message rates, the private information leakage to the fusion center, the equivocation at Eve and the distortion.

To gain design insights, we first study an important special case where there is only one transmitter (by setting $\mathcal{X}_2 = \emptyset$). This case recovers the basic function computation problem [13] but with additional privacy and secrecy considerations. We fully characterize the regions of the involved parameters for both the lossless and the lossy function computation cases. The results demonstrate that there exist tradeoffs among these parameters. For example, given the distortion level, the message rate and privacy leakage can be simultaneously optimized but the secrecy level of sources at Eve may not be simultaneously maximized. In addition, we show that, even though the lossless case has a more stringent constraint than that of the lossy case with distortion being zero, the obtained result for the lossless case is equivalent to that of the special case of the lossy case. The results obtained in this part have been presented in [1] and [2].

Using the understanding from the single transmitter case, we then extend the study to the scenario with two transmitters. We first derive both an outer bound and an inner bound on the corresponding region for the lossless case. These outer and inner bounds have the same form but with different range for auxiliary random variables involved. The obtained results recover many existing results [17], [30], and show that there exist tradeoffs among different parameters involved in the model. Furthermore, the techniques used in the lossless case are generalized into the lossy case. We also provide both an outer bound and an inner bound on the corresponding region. Similar to the lossless case, the obtained outer and inner bounds have the same form but with different range for auxiliary random variables involved.

We now briefly review some interesting related works. In [31], Neri studied an extension of Shanon's secrecy system. In the model considered in [31], the transmitter and the receiver, each observing a component of two correlated sequences, share a common secret key. There is also a wiretapper who has a degraded side information. To enable the receiver to decode the transmitter's source sequence within a given distortion level while keeping the equivocation of the source at the wiretapper larger than a given value, the transmitter can send a message to the receiver over a noisy channel and the wiretapper also observes a more noisy output. Reference [31] characterizes the achievable region of five related metrics including the equivocation, the key rate, the distortion level, etc. Similar rate distortion problems for secrecy systems with common secret keys are further considered under different models [32], [33]. Related problems are also studied for scenarios without shared secret keys [34]–[38]. For example, in [34], the transmitter has two correlated source sequences, and it is allowed to send a message as a function of these two sequences to the receiver so that the receiver can decode one of the sequences within a given distortion level while keeping the equivocation of the other sequences at the receiver larger than a given value. Reference [34] investigates the relationship among the message rate, the distortion level and the equivocation. A common theme in these papers is that they study the relationship among different parameters such as message rates, equivocation level of the intended sources at the eavesdroppers, and the distortion level between the decoded sequences and the intended sources, etc. In this respect, our paper is related to these very interesting papers. One pivotal difference between the setups in these papers and the setup in our paper is that the decoder in our setup is only interested in a function of the source sequence (not the source sequence itself) and the distortion level in our paper is measured on the intended function.

The remainder of this paper is organized as follows. In Section II, we introduce the system model. In Section III, we consider the special case where there is only one transmitter. The scenario with two transmitters is analyzed in Section IV. In Section V, we provide proofs of results presented in this paper. In Section VI, we offer our concluding remarks.

II. System Model

As illustrated in Fig. 1, in the considered model, two legitimate terminals, Alice and Bob, are connected to the

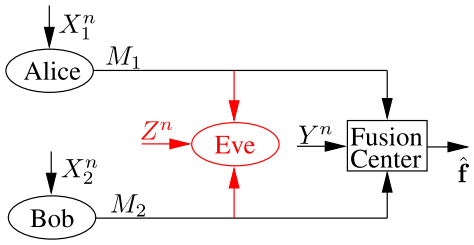

Fig. 1. System model: The fusion center would like to compute a function f of (X_1^n, X_2^n, Y^n). Alice and Bob are connected to the fusion center via public noiseless channels, which Eve has full access to.

fusion center via two public noiseless channels in the presence of an eavesdropper Eve who has full access to the public channels, and there is no link between Alice and Bob. Alice, Bob, the fusion center and Eve observe n-length correlated source sequences X_1^n, X_2^n, Y^n and Z^n respectively. These sequences are generated according to a given probability mass function (PMF) $P_{X_1X_2YZ}$:

$$\Pr\{X_1^n, X_2^n, Y^n, Z^n\} = \prod_{i=1}^{n} P_{X_1X_2YZ}(X_{1i}, X_{2i}, Y_i, Z_i), \quad (1)$$

where (X_1, X_2, Y, Z) take values from finite alphabets $(\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Z})$ respectively.

The fusion center would like to compute a function $\mathbf{f}(X_1^n, X_2^n, Y^n)$ that consists of component-wise functions of $\{X_{1i}, X_{2i}, Y_i\}_{i=1}^n$, and $\mathbf{f}(X_1^n, X_2^n, Y^n)$ can be written as

$$\mathbf{f}(X_1^n, X_2^n, Y^n) := \{f(X_{1i}, X_{2i}, Y_i)\}_{i=1}^n.$$

$\mathbf{f}(X_1^n, X_2^n, Y^n)$ is denoted by $\mathbf{f}$ in short and $f(X_{1i}, X_{2i}, Y_i)$ is denoted by f_i for $i \in [1:n]$. Thus, we rewrite $\mathbf{f}(X_1^n, X_2^n, Y^n)$ as $\mathbf{f} := f^n$.

Define M_1 and M_2 as (stochastic) functions of X_1^n and X_2^n, respectively. To facilitate the computation of $\mathbf{f}$ at the fusion center, Alice will send M_1 and Bob will send M_2 to the fusion center via the public channels. After receiving these messages, the fusion center computes an estimated value $\hat{\mathbf{f}}$ of $\mathbf{f}$, based on M_1, M_2 and Y^n.

In the considered model, Alice and Bob have privacy constraints in the sense that they would like to minimize privacy leakage to the fusion center and Eve about their observations while still enabling the fusion center to compute the function of interest. We use $\frac{1}{n} I(X_1^n, X_2^n; M_1, M_2|Y^n)$ to measure additional private information leakage about (X_1^n, X_2^n) to the fusion center. As $I(X_1^n, X_2^n; M_1, M_2|Y^n) = H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n)$, this quantity measures additional information about (X_1^n, X_2^n) that the fusion center learns from (M_1, M_2), and hence is the privacy price we pay in order to compute $\mathbf{f}$. We use $\frac{1}{n} H(X_1^n, X_2^n|M_1, M_2, Z^n)$ to measure the equivocation of (X_1^n, X_2^n) at Eve.

Definition 1. *Given an arbitrary random variable alphabet $\mathcal{F}$ and its reconstruction alphabet $\hat{\mathcal{F}}$, the distortion measure is a mapping*

$$d : \mathcal{F} \times \hat{\mathcal{F}} \to [0, \infty),$$

and the distortion between given sequences f^n and $\hat{f}^n$ is measured as

$$d(f^n, \hat{f}^n) = \sum_{i=1}^{n} d(f_i, \hat{f}_i).$$

Definition 2. *Given a per-letter distortion measure mapping d, a tuple $(R_1, R_2, D, \Delta_1, \Delta_2)$ is said to be* achievable *if $\forall \epsilon > 0$, there exists an $n(\epsilon) \in \mathbb{N}$ and a sequence of $(n, R_1, R_2, D, \Delta_1, \Delta_2)$ codes such that $\forall n > n(\epsilon)$*

$$\frac{1}{n} E[d(\mathbf{f}, \hat{\mathbf{f}})] \le D + \epsilon, \quad (2)$$

$$\frac{1}{n} H(M_i) \le R_i + \epsilon, \ i = 1, 2, \quad (3)$$

$$\frac{1}{n} I(X_1^n, X_2^n; M_1, M_2|Y^n) \le \Delta_1 + \epsilon, \quad (4)$$

$$\frac{1}{n} H(X_1^n, X_2^n|M_1, M_2, Z^n) \ge \Delta_2 - \epsilon. \quad (5)$$

Here, (2) indicates that the average distortion between the estimated value $\hat{\mathbf{f}}$ and the true value $\mathbf{f}$ is less than a given positive parameter D, (3) measures the transmitted message rates at Alice and Bob respectively, (4) implies that the extra privacy leakage of (X_1^n, X_2^n) to the fusion center is less than Δ_1, and (5) measures the joint equivocation of (X_1^n, X_2) at Eve's side.

Remark 1. *As $I(X_1^n, X_2^n; M_1, M_2|Y^n) = H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n)$, the privacy constraint and the secrecy constraint have similar formulations. Another possible problem formulation is to change the secrecy constraint to the equivocation of the function at Eve, i.e., $\frac{1}{n} H(\mathbf{f}(X_1^n, X_2^n, Y^n)|M_1, M_2, Z^n) \ge \Delta_2 - \epsilon$. However, it is difficult to characterize the secrecy relationship between $\mathbf{f}$ and (M_1, M_2, Z^n), as the secrecy of $\mathbf{f}$ also depends on its specific formulation. It will be of interest to consider this alternative formation in the future study.*

In Definition 2, in the case when $D = 0$, we replace (2) with the following condition:

$$\Pr\{\mathbf{f} \neq \hat{\mathbf{f}}\} \le \epsilon, \quad (6)$$

while keeping the inequalities (3)-(5) unchanged. For this case, we rewrite the tuple $(n, R_1, R_2, D = 0, \Delta_1, \Delta_2)$ as $(n, R_1, R_2, \Delta_1, \Delta_2)$ in short. Obviously, the constraint defined by (6) is stricter than that defined by (2). We refer the case when $D = 0$ with constraints defined by (3)-(6) as *lossless function computation*, and the case with constraints defined by (2)-(5) as *lossy function computation*. The lossless function computation case can be viewed as a special case of the lossy function computation case, but with a stricter constraint, thus it deserves an independent investigation.

Definition 3. *The set of all achievable tuple $(R_1, R_2, D, \Delta_1, \Delta_2)$ is defined as*:

$$\mathcal{S} := \{(R_1, R_2, D, \Delta_1, \Delta_2) \in \mathbb{R}_+^5 : (R_1, R_2, D, \Delta_1, \Delta_2) \text{ is achievable } \}.$$

Our goal is to characterize the region $\mathcal{S}$.

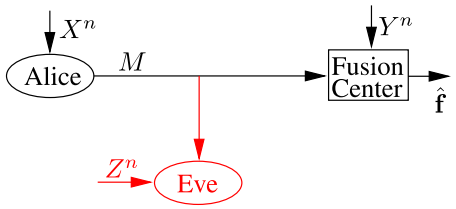

Fig. 2. The case with $\mathcal{X}_2 = \emptyset$: The fusion center would like to compute a value as a function of sequences X^n and Y^n. Alice is connected to the fusion center via a public noiseless channel, which Eve has full access to.

III. A Special Case With $\mathcal{X}_2 = \emptyset$

In this section, we study a special case when $\mathcal{X}_2 = \emptyset$. In this case, for presentation convenience, we denote X_1 by X, and M_1 by M. The model is shown in Fig. 2.

A. Lossless Function Computation

In this part, we study the lossless function computation case. Before proceeding to the main results, we introduce the following definition (similar to the definition introduced in [13, Section V. B]) that will simplify the presentation of results in the sequel.

Definition 4. *A random variable U is said to be* admissible *with respect to random variables X, Y and function f (we may write U is admissible in short), if it satisfies*

1) $U \to X \to Y$;
2) *U and Y determine f, i.e., $H(f|U, Y) = 0$.*

Furthermore, a sequence u^n is said to be an admissible sequence with respect to x^n and y^n if $\forall i \in [1 : n]$, (u_i, y_i) determine $f(x_i, y_i)$.

Here, condition 1) denotes that random variables U, X and Y form a Markov chain in this order. Condition 2) is equivalent to the condition that there exists a deterministic function g such that $g(U, Y) = f(X, Y), \forall (X, Y)$ with $P_{XY}(X, Y) > 0$, according to [30, Chapter 2].

When Eve observes the public discussion, Eve can utilize it along with Z^n to infer the information about the sequence X^n, thus, the equivocation of X^n at Eve reduces. We have the following result.

Theorem 1. *The achievable tuple set $\mathcal{S}$ for the case when Eve has side information is given by*

$$\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R \geq I(X; U) - I(Y; U), \tag{7}$$
$$\Delta_1 \geq I(X; U|Y), \tag{8}$$
$$\Delta_2 \leq H(X|U, Z) + [I(Y; U|V) - I(Z; U|V)]^+, \tag{9}$$
$$\text{for some admissible } U \text{ and a r.v. } V \text{ with } V \to U \to X \to (Y, Z)\Big\}, \tag{10}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 2$ and $|\mathcal{V}| \leq (|\mathcal{X}| + 1)(|\mathcal{X}| + 2)$.

Proof: Please see Section V-A. ∎

To facilitate the understanding, we illustrate the results in Theorem 1 for the special case when $\mathcal{Z} = \emptyset$ (i.e., Eve has no side information), for which we have the following corollary.

Corollary 1. *The achievable tuple set $\mathcal{S}$ in the case when $\mathcal{Z} = \emptyset$ is*

$$\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R \geq I(X; U|Y), \tag{11}$$
$$\Delta_1 \geq I(X; U|Y), \tag{12}$$
$$\text{and } \Delta_2 \leq H(X) - I(X; U|Y), \tag{13}$$
$$\text{for some admissible } U \text{ w.r.t. } X, Y \text{ and } f\Big\}, \tag{14}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 2$.

Intuitively, for the case when $\mathcal{Z} = \emptyset$, to reduce the additional information leakage to the fusion center and to increase the equivocation at Eve, Alice should reduce the information of X^n contained in the public message. Obviously, the set of all possible random variables U is not empty: X belongs to this set. In addition, from Corollary 1, we can see that (R, Δ_1, Δ_2) can be optimized simultaneously. In particular, when R achieves its optimal value denoted by R^*, the values of Δ_1 and Δ_2 can be R^* and $H(X) - R^*$ respectively, which are the corresponding optimal values. In other words, there exists a U that achieves lower bounds on R and Δ_1, and the upper bound for Δ_2, simultaneously. Set

$$U^* = \arg \min_{U \text{ is admissible}} I(X; U|Y), \tag{15}$$

then the set $\mathcal{S}$ in Corollary 1 can be rewritten as

$$\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R \geq I(X; U^*|Y), \Delta_1 \geq I(X; U^*|Y), \text{and } \Delta_2 \leq H(X) - I(X; U^*|Y)\Big\}.$$

In addition, given PMF P_{XY} and function $f(X, Y)$, the range of U can be written in an alternative manner by introducing conditional characteristic graph as shown [13]. Reference [13] focuses on characterizing the least message rate and does not take Δ_1 and Δ_2 into consideration. As a special case when we only care about R, the result in Corollary 1 is consistent with the result obtained in [13]. We now consider a simple example.

Example 1: for $X, Y \in \{1, 2, 3\}$, define

$$P_{XY}(x, y) = \begin{cases} \frac{1}{6}, & \text{if } x \neq y \\ 0, & \text{if } x = y \end{cases} \text{and } f(x, y) = \begin{cases} 1, & \text{if } x > y \\ 0, & \text{if } x < y \end{cases},$$

then, the optimal U^* (by solving (15), or refer to [13]) is given by

$$P_{U^*|X}(0|1) = 1, \ P_{U^*|X}(0|2) = \frac{1}{2}, \ P_{U^*|X}(0|3) = 0, \tag{16}$$

with $u^* \in \{0, 1\}$. We can easily calculate that $I(X; U^*|Y) \approx 0.541$ and $H(X) - I(X; U^*|Y) \approx 1.044$, thus the corresponding achievable region for this example is given by

$$\mathcal{S} = \Big\{(R, \Delta_1, \Delta_2) : R \geq 0.541, \Delta_1 \geq 0.541, \Delta_2 \leq 1.044\Big\}.$$

For the case when $\mathcal{Z} \neq \emptyset$, the existence of side-information Z^n provides more information to Eve about X^n. Thus, it is necessary to introduce an additional random variable V that

serves as stochastic encoding to confuse Eve. Compared with the result in Corollary 1, there exists a tradeoff among the tuple (R, Δ_1, Δ_2): in general, there does not exist an optimal solution (U^*, V^*) that minimizes R and Δ_1, and maximizes Δ_2 simultaneously.

The result in Theorem 1 can also be simplified if the source random variables satisfy the Markov chain relationship $X \to Y \to Z$.

Corollary 2. *If $X \to Y \to Z$ holds, the achievable tuple set $\mathcal{S}$ is given by*

$$\mathcal{S} = \Big\{ (R, \Delta_1, \Delta_2) : R \geq I(X; U|Y), \tag{17}$$
$$\Delta_1 \geq I(X; U|Y), \tag{18}$$
$$\Delta_2 \leq H(X|Z) - I(X; U|Y), \tag{19}$$
$$\text{for some admissible } U \Big\},$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 2$.

Proof. For the notation convenience, under the condition that $X \to Y \to Z$ holds, we denote the region stated in Theorem 1 as $\hat{\mathcal{S}}$ and the region in the corollary as $\tilde{\mathcal{S}}$. On the one hand, we have

$$\begin{aligned} &H(X|Z) - I(X; U|Y) \\ &\quad = H(X|Z) - I(X; U|Y, Z) \\ &\quad = H(X|Z) - I(Y, X; U|Z) + I(U; Y|Z) \\ &\quad = H(X) - I(X; Z) - I(X; U|Z) + I(U; Y|Z) \\ &\quad = H(X) - I(X; U, Z) + I(U; Y|Z) \\ &\quad = H(X|U, Z) + I(Y; U) - I(Z; U). \end{aligned} \tag{20}$$

Using this equation and setting $\mathcal{V} = \emptyset$ in (9), we have that (9) is equivalent to (19), and we can obtain $\tilde{\mathcal{S}}$ from $\hat{\mathcal{S}}$. Thus, we have $\tilde{\mathcal{S}} \subseteq \hat{\mathcal{S}}$.

On the other hand, we can show that $\hat{\mathcal{S}} \subseteq \tilde{\mathcal{S}}$. Towards this end, it suffices to show that $H(X|U, Z) + [I(Y; U|V) - I(Z; U|V)]^+ \leq H(X|U, Z) + I(Y; U) - I(Z; U)$, which is equivalent to

$$\begin{aligned} &I(Y; U|V) - I(Z; U|V) \leq I(Y; U) - I(Z; U) \\ \Leftrightarrow\ &I(Y; V) \geq I(Z; V). \end{aligned}$$

And that $I(Y; V) \geq I(Z; V)$ is true due to the Markov chain $V \to U \to X \to Y \to Z$. Hence, we have $\hat{\mathcal{S}} = \tilde{\mathcal{S}}$, and this completes the proof. □

If the Markov chain $X \to Y \to Z$ holds, then Y has more information about X than Z has. Hence, if enough information is hidden from the fusion center, then the equivocation on Eve will also be maximized. Equivalently, similar to Corollary 1, there is an optimal U achieving the minimal values for R, Δ_1 and the maximal value for Δ_2 simultaneously.

Example 2: for $X, Y \in \{1, 2, 3\}$ and $Z \in \{0, 1\}$, suppose P_{XY} and $f(X, Y)$ are the same as defined in *Example 1*, and $P_{Z|Y}$ is defined as follows ($X \to Y \to Z$):

$$P_{Z|Y}(0|1) = \frac{1}{2}, \ P_{Z|Y}(0|2) = \frac{1}{3}, \ P_{Z|Y}(0|3) = \frac{2}{3},$$

then, the optimal U^* will be the same as defined in (16), and we can calculate that $H(X|Z) \approx 1.572$. Thus, the achievable region for (R, Δ_1, Δ_2) is given by

$$\begin{aligned} \mathcal{S} = \Big\{ &(R, \Delta_1, \Delta_2) : R \geq 0.541, \\ &\Delta_1 \geq 0.541, \\ &\Delta_2 \leq 1.031 \}. \end{aligned}$$

B. Lossy Function Computation

In this section, we focus on the lossy function computation case, i.e. $D > 0$. In this case, the fusion center is not required to recover the value of function $\mathbf{f}$ exactly, it only needs to compute $\mathbf{f}$ within a prefixed allowed distortion level for a given distortion metric. This relaxed requirement allows us to reduce the message rate and the privacy leakage.

Given a distortion measure mapping d on the alphabets of $\mathbf{f}$ and its reconstruction, we have the following result.

Theorem 2. *Given distortion measure mapping d, the achievable tuple set $\mathcal{S}$ for the coding of lossy function computation is given by*

$$\mathcal{S} = \Big\{ (R, D, \Delta_1, \Delta_2) : R \geq I(X; U) - I(Y; U), \tag{21}$$
$$D \geq E[d(f(X, Y), g(U, Y))], \tag{22}$$
$$\Delta_1 \geq I(X; U|Y), \tag{23}$$
$$\Delta_2 \leq H(X|U, Z) + [I(Y; U|V) - I(Z; U|V)]^+, \tag{24}$$
$$\text{for some function } g \text{ and r.v. } U, V \text{ with}$$
$$V \to U \to X \to (Y, Z) \Big\}, \tag{25}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 3$ and $|\mathcal{V}| \leq (|\mathcal{X}| + 1)(|\mathcal{X}| + 3)$.

Proof: Please see Section V-B. ■

We note that, although there is a function g in the description of the region, the form of g is implicitly determined by the choice of U. In particular, for any PMF P_{XYZUV} and function f, we can always find an optimal function g^* as follows:

$$g^*(U, Y) = \arg\min_g E[d(f(X, Y), g(U, Y))].$$

Consider the case with hamming distance as an example. Here, we take the function f as a variable (denoted by F) and its value as to realization (denoted by f).

$$\begin{aligned} E[d(F, g(U, Y))] &= \sum_{f,u,y} P_{FUY}(f, u, y) d(f, g(u, y)) \\ &\geq 1 - \sum_{u,y} P_{FUY}(\hat{f}, u, y), \end{aligned}$$

where $\hat{f} := \arg\max_f P_{F|UY}(f|u, y)$. Thus, $\forall (u, y) \in \mathcal{U} \times \mathcal{Y}$, we can obtain the optimal function g as

$$g^*(u, y) := \arg\max_f P_{F|UY}(f|u, y). \tag{26}$$

When P_{XYZUV} and function f are given, the PMF P_{FUY} is given and it is straightforward to find the solution to (26).

Note that, unlike the lossless case, the random variable U here is not required to be admissible w.r.t (X, Y) and f anymore. As shown in [13], in the lossless case, there are

many scenarios where the fusion center needs to decode X^n exactly so that it can compute $\mathbf{f}$. However, when a certain amount of distortion is allowed, there always exists random variable U other than X, such that the decoder only needs to decode the sequence U^n. This sequence serves as distortion mapping of X^n, which helps in increasing the equivocation of X^n at Eve and reducing the privacy leakage to the fusion center.

A special case of our setup is equivalent to the setup considered in Theorem 3 of [37], and the obtained result is consistent with [37, Theorem 3]. In particular, if we set $\mathbf{f}(X^n, Y^n) := X^n$ and consider the region of (R, D, Δ_2) only in our setup, then it is equivalent to the setup considered in Theorem 3 of [37]. We can easily verify that (21) is equivalent to equation (7) of [37] and (22) is equivalent to equation (8) of [37]. We only need to verify that (24) is equivalent to (9) of [37]. To make it clearer, we restate (9) of [37] using the corresponding notation in this paper:

$$\Delta_2 \leq H(X|U,Y) + I(X;Y|V) - I(X;Z|V).$$

It suffices to show that $H(X|U,Y) + I(X;Y|V) - I(X;Z|V) = H(X|U,Z) + I(Y;U|V) - I(Z;U|V)$, which is true as we have

$$\begin{aligned}
& H(X|U,Y) + I(X;Y|V) - I(X;Z|V) \\
&\qquad = H(X|U,Z) + I(Y;U|V) - I(Z;U|V) \\
\Leftrightarrow\ & H(X|U,Y) - H(Y|X,V) + H(Z|X,V) \\
&\qquad = H(X|U,Z) - H(Y|U,V) + H(Z|U,V) \\
\Leftrightarrow\ & H(X|U,Y) - H(Y|X) + H(Z|X) \\
&\qquad = H(X|U,Z) - H(Y|U) + H(Z|U) \\
\Leftrightarrow\ & H(X|U,Y) - H(X|U,Z) \\
&\qquad = H(Y|X) - H(Y|U) + H(Z|U) - H(Z|X) \\
\Leftrightarrow\ & H(X|U,Y) - H(X|U,Z) \\
&\qquad = -I(X;Y|U) + I(X;Z|U) \\
\Leftrightarrow\ & H(X|U,Y) - H(X|U,Z) \\
&\qquad = H(X|U,Y) - H(X;|U,Z). \qquad (27)
\end{aligned}$$

Comparing the results in Theorems 1 and 2, we observe that the region given in Theorem 2, when $D = 0$, is the same as that in Theorem 1, even though the requirement in the lossless function computation case is stricter than that in the lossy case, i.e., (6) is stricter than that of setting $D = 0$ to (2). In addition, similar to Corollary 2, we have the following corollary when $X \to Y \to Z$ holds in the lossy function computation case.

Corollary 3. *If $X \to Y \to Z$ holds, the achievable tuple set $\mathcal{S}$ in the lossy function computation case is given by*

$$\begin{aligned}
\mathcal{S} = \Big\{ & (R, D, \Delta_1, \Delta_2) : R \geq I(X;U|Y), && (28)\\
& D \geq E[d(f(X,Y), g(U,Y))], && (29)\\
& \Delta_1 \geq I(X;U|Y), && (30)\\
& \Delta_2 \leq H(X|Z) - I(X;U|Y), && (31)\\
& \text{for some function } g \text{ and r.v. } U \text{ with} \\
& U \to X \to Y \to Z \Big\}, && (32)
\end{aligned}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 3$.

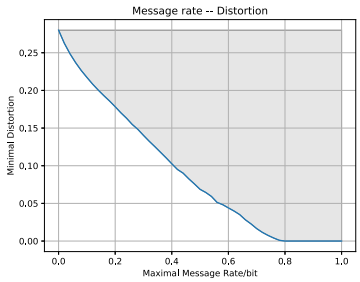

Fig. 3. Relationship between maximal message rate R and minimal computed function distortion.

The proof follows similar steps as that in the derivative of Corollary 2, thus is omitted here. From (28) to (31), we can see that there exists a trade-off among these parameters: for given P_{XYZ}, Δ_2 linearly decreases as R (or Δ_1) increases, but D is not generally linear in it on the boundary. Thus, there may not exist an optimal U^* that achieves optimal values for R, D, Δ_1 and Δ_2 simultaneously. We now give an example to illustrate the tradeoff.

Example 3: For $X, Y, Z \in \{0,1\}$, suppose $X \to Y \to Z$, $P_X(0) = \frac{2}{5}$, $P_X(1) = \frac{3}{5}$, $P_{Y|X}$ and $P_{Z|Y}$ are:

$$P_{Y|X} = \begin{bmatrix} \frac{4}{5} & \frac{1}{5} \\ \frac{1}{3} & \frac{2}{3} \end{bmatrix}, \quad P_{Z|Y} = \begin{bmatrix} \frac{2}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{bmatrix},$$

$\mathbf{f}(X^n, Y^n) = X^n \oplus Y^n$, and the distortion is measured by Hamming distance. Fig. 3 illustrates the relationship between R and D. In this example, we only plot the relationship between R and D, as the values of Δ_1 and Δ_2 can be determined by R. We obtain this figure by numerically computing (28) and (29). The right-upper region is the achievable region for (R, D): when $R = 0$ (i.e., no message transmitted from Alice), the minimal distortion rate is 0.28; when $R \geq 0.80$ (note that $H(X|Y) = 0.81$) the minimal distortion is close to 0.

Note that the minimum values of the private information leakage rate and the message rate are always the same for the single transmitter case. The reason is that, for any variable U achieving the region boundary, there exists a coding scheme so that the transmitted message M is a function of X^n, and it is independent with Y^n (so are the transmitted messages in the coding schemes of our proofs). Thus, the private information leakage rate is the same as the transmitter information rate.

IV. The Case When $\mathcal{X}_2 \neq \emptyset$

In this section, we study the case when $\mathcal{X}_2 \neq \emptyset$. Despite being much more complicated than the case when $\mathcal{X}_2 = \emptyset$, the techniques developed in the previous section can be generalized to this case.

We first consider the lossless function computation case, for which we have both inner and outer bounds on the region of achievable tuples as follows.

Theorem 3. *(Converse) For lossless function computation at the fusion center, if the tuple $(R_1, R_2, \Delta_1, \Delta_2)$ is achievable, then there exist auxiliary random variables (U_1, V_1) and (U_2, V_2) with $|\mathcal{U}_1| \leq |\mathcal{X}_1| + 4, |\mathcal{V}_1 \leq (|\mathcal{X}_1| + 1)(|\mathcal{X}_1| + 4)$,*

$|\mathcal{U}_2| \leq |\mathcal{X}_2| + 4$, *and* $|\mathcal{V}_2| \leq (|\mathcal{X}_2| + 1)(|\mathcal{X}_2| + 4)$, *for which* $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ *and* $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ *form Markov chains in the indicated orders, and*

$$R_1 \geq I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1) - I(V_1; V_2|Y, X_1) - I(U_1; U_2|X_1, Y, V_1), \quad (33)$$

$$R_2 \geq I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) - I(V_1; V_2|Y, X_2) - I(U_1; U_2|X_2, Y, V_2), \quad (34)$$

$$R_1 + R_2 \geq I(V_1; X_1|Y) + I(V_2; X_2|Y, V_1) + I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2), \quad (35)$$

$$\Delta_1 \geq I(X_1, X_2; U_1, U_2|Y), \quad (36)$$

$$\Delta_2 \leq H(X_1, X_2|U_1, U_2, Z) + \left[I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)\right]^+, \quad (37)$$

$$H(f|U_1, U_2, Y) = 0. \quad (38)$$

(Achievability) Furthermore, for random variables (U_1, V_1) *and* (U_2, V_2) *satisfying* $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$ *and* $H(f|U_1, U_2, Y) = 0$, *then the tuple* $(R_1, R_2, \Delta_1, \Delta_2)$ *subject to* (33)-(37) *is achievable.*

Proof: Please see Section V-C. ∎

In general, the converse and the achievable bounds do not match because the region of U_1, V_1 and U_2, V_2 defined by $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ and $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ in the converse bound is larger than that defined by $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$ in the achievability bound. Note that, the minus terms on the right-hand sides of (33) and (34) are zero if $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$, since we have

$$(V_1, U_1) \to X_1 \to (Y, U_2, V_2),$$
$$(V_2, U_2) \to X_2 \to (Y, U_1, V_1),$$

in this case.

By setting $\mathcal{V}_1 = \mathcal{V}_2 = \emptyset$, we observe that the achievability result of the message rate region defined by (33)-(35) and (38) recovers the inner bound obtained in [17, Prop. 1]. In addition, it is consistent with a special case of the result obtained in [19, Theorem 2] when the rooted directed tree involves with only three nodes: one root and two children.

Given $P_{U_1V_1U_2V_2X_1X_2YZ}$, the main idea of our achievable scheme is that there exist auxiliary sequences U_1^n, V_1^n and U_2^n, V_2^n such that $\mathbf{f}(X_1^n, X_2^n, Y^n) = \hat{\mathbf{f}}(U_1^n, U_2^n, Y^n)$ if $(R_1, R_2, \Delta_1, \Delta_2)$ is achievable. Thus, the function $\mathbf{f}$ will be correctly computed at the fusion center as long as it can correctly decodes (U_1^n, U_2^n), and (33)-(35) define the region of (R_1, R_2), such that (U_1^n, U_2^n) can be correctly decoded with some scheme. And sequences V_1^n, V_2^n are used to increase the equivocation of (X_1^n, X_2^n) at Eve.

Under certain scenarios where we need to correctly decode X_1^n and X_2^n, i.e., f is an invertible function with respect to X_1 and X_2: $U_1 = X_1$, $U_2 = X_2$ [17], and when we only care about the region of (R_1, R_2), we have the following corollary.

Corollary 4. *Given* $P_{X_1X_2Y}$, *sequences* (X_1^n, X_2^n) *can be correctly decoded, if and only if*

$$R_1 \geq H(X_1|Y) - I(X_1; X_2|Y)$$
$$R_2 \geq H(X_2|Y) - I(X_1; X_2|Y)$$
$$R_1 + R_2 \geq H(X_1|Y) + H(X_2|Y) - I(X_1; X_2|Y).$$

Corollary 4 recovers the result in [17, Rate Region - Invertible Function]. In addition, it recovers the distributed source coding problem when $\mathcal{Y} = \emptyset$ as well, and the result is consistent with the Slepian-Wolf coding theorem [30, Chap. 15].

For the lossy function computation case with a given distortion metric d, we have the following result regarding the tradeoffs among message rates, information leakage, equivocation and distortion.

Theorem 4. *(Achievability) Given a distortion mapping* d, *the tuple* $(R_1, R_2, D, \Delta_1, \Delta_2)$ *is achievable if*

$$R_1 \geq I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1) - I(V_1; V_2|Y, X_1) - I(U_1; U_2|X_1, Y, V_1), \quad (39)$$

$$R_2 \geq I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) - I(V_1; V_2|Y, X_2) - I(U_1; U_2|X_2, Y, V_2), \quad (40)$$

$$R_1 + R_2 \geq I(V_1; X_1|Y) + I(V_2; X_2|Y, V_1) + I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2), \quad (41)$$

$$\Delta_1 \geq I(X_1, X_2; U_1, U_2|Y), \quad (42)$$

$$\Delta_2 \leq H(X_1, X_2|U_1, U_2, Z) + \left[I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)\right]^+, \quad (43)$$

$$D \geq E\left[d\left(f(X_1, X_2, Y), g(U_1, U_2, Y)\right)\right], \quad (44)$$

for some function g *and auxiliary random variables* U_1, V_1 *and* U_2, V_2 *with* $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$.

(Converse) If the tuple $(R_1, R_2, \Delta_1, \Delta_2)$ *is achievable, there exist some function* g *and auxiliary random variables,* (U_1, V_1) *and* (U_2, V_2) *with* $|\mathcal{U}_1| \leq |\mathcal{X}_1| + 4$, $|\mathcal{V}_1 \leq (|\mathcal{X}_1| + 1)(|\mathcal{X}_1| + 4)$, $|\mathcal{U}_2| \leq |\mathcal{X}_2| + 4$, *and* $|\mathcal{V}_2| \leq (|\mathcal{X}_2| + 1)(|\mathcal{X}_2| + 4)$, *for which* $V_1 \to U_1 \to X_1 \to (X_2, Y, Z)$ *and* $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ *form Markov chains in the indicated orders, such that* (39)-(44) *hold.*

Proof: Please see Section V-D. ∎

Similar to the relationship in Theorem 3, the region defined in the converse does not match the region defined in the achievability. For given (V_i^n, U_i^n, X_i^n), $i \in \{1, 2\}$ and Y^n, Z^n, which are generated by $P_{U_1V_1U_2V_2X_1X_2YZ}$, (39)-(41) guarantee that there exists a coding scheme such that the fusion center can correctly decode $(V_1^n, U_1^n, V_2^n, U_2^n)$, thus the privacy information leakage is no less than $I(X_1^n, X_2^n; U_1^n, U_2^n|Y^n)$. The first term in the right-hand side of (43) measures the secrecy of sources as if (U_1^n, U_2^n) were provided to Eve, and the increased secrecy rate introduced by the second term is due to the presence of (V_1^n, V_2^n), whose purpose is to prevent Eve from learning more information about (X_1^n, X_2^n). When $D = 0$, Theorem 4 requires that $E(d(f(X_1, X_2, Y), g(U_1, U_2, Y))) = 0$,

which implies $H(f|U_1, U_2, Y) = 0$. Thus, we conclude that the achievability and converse regions provided in Theorem 3 can be viewed as a special case of the regions characterized in Theorem 4.

V. Proofs

In this paper, we use the term *typicality* as defined in [39, Chapter 2], i.e., given a small number $\epsilon > 0$, a sequence X^n is said to be typical if

$$|\pi(x|X^n) - P_X(x)| \leq \epsilon P_X(x), \forall x \in \mathcal{X}, \tag{45}$$

where $\pi(x|X^n) := |\{i : X_i = x\}|/n$ is the empirical PMF of X^n.

We first have the following lemma that is very useful for achievability proofs in the sequel.

Lemma 1. *Given P_{UXY}, where U is admissible, and function f, suppose x^n is a typical sequence and Y^n is generated according to $\Pi_i^n P_{Y|X}(y_i|x_i)$, then U^n is an admissible sequence if it is jointly typical with x^n according to P_{UX}.*

Proof. Given $X = x$, we only need to consider realizations $y \in \mathcal{Y}$ with $P_{\{XY\}}(x, y) > 0$. According to Definition 4, we have

$$\Pr\{f(x, Y) = g(U, Y)\} = 1, \tag{46}$$

which is equivalent to

$$\sum_{u \in \mathcal{U}} P_{U|X}(u|x)\Pr\{f(x, Y) = g(u, Y)\} = 1. \tag{47}$$

This means that for all $u \in \mathcal{U}$, $\Pr\{f(x, Y) = g(u, Y)\} = 1$ if $P_{U|X}(u|x) \neq 0$. Denote the support of the conditional PMF $P_{U|X}(U|x)$ by

$$S_{P_{UX}}(x) := \{u \in \mathcal{U} : P_{U|X}(u|x) > 0\}. \tag{48}$$

The typicality of x^n and U^n guarantees that the probability of $U_i \notin S_{P_{UX}}(x_i)$ is zero, since $\forall U_i \notin S_{P_{UX}}(x_i)$,

$$P_{UX}(U_i, x_i) = P_X(x)P_{U|X}(U_i|x_i) = 0, \tag{49}$$

and

$$\begin{aligned} &|\pi((U_i, x_i)|(U^n, x^n)) - P_{UX}(U_i, x_i)| \leq \epsilon P_{UX}(U_i, x_i) \\ &\Leftrightarrow | \ \ \pi((U_i, x_i)|(U^n, x^n))| \leq 0. \end{aligned} \tag{50}$$

Thus, we can conclude that U^n is admissible. □

Furthermore, throughout the paper, we will make extensive use of the following equality in the converse proof.

Lemma 2 (Lemma 4.1 of [40])**.** *For arbitrary RVs U, V and sequences of RVs Y^n, Z^n we have*

$$\begin{aligned} &I(U; Y^n|V) - I(U; Z^n|V) \\ &= \sum_{i=1}^{n} \Big[I(U; Y_i|Y^{i-1}, Z_{i+1}^n, V) - I(U; Z_i|Y^{i-1}, Z_{i+1}^n, V) \Big]. \end{aligned}$$

Now, we provide detailed proofs of the theorems presented in this paper.

A. Proof of Theorem 1

Achievability:

Given PMF $P_{XYZ}P_{U|X}P_{V|U}$ with U being admissible, the case when $I(Y; U|V) - I(Z; U|V) \leq 0$ is trivial. Without loss of generality, we assume that $I(Y; U|V) - I(Z; U|V) > 0$. For any sufficiently small value $\epsilon > 0$, we will show that the tuple (R, Δ_1, Δ_2) with

$$\begin{aligned} R &= I(X; U) - I(Y; U) + 4\epsilon, \\ \Delta_1 &= I(X; U|Y) + 2\epsilon, \\ \Delta_2 &= H(X|U, Z) + [I(Y; U|V) - I(Z; U|V)] - 5\epsilon, \end{aligned}$$

is achievable.

1) **Codebook ($\mathcal{C}$) construction:** Randomly and independently generate 2^{nR_0} sequences V^n according to $\prod_{i=1}^n P_V(v_i)$, and assign each V^n into 2^{R_1} bins which are indexed by M', using a uniform distribution. We use $b(M')$ to denote bin M'; For each generated sequence V^n, randomly and independently generate 2^{nR_2} sequences U^n according to $\prod_{i=1}^n P_{U|V}(u_i|v_i)$, and assign each U^n into 2^{nR_3} bins indexed by M'', using a uniform distribution. We use $b_{V^n}(M'')$ to denote the corresponding bin of sequences U^n. In addition, we set
$$R_0 = I(X; V) + \epsilon, \tag{51}$$
$$R_1 = I(X; V) - I(Y; V) + 2\epsilon, \tag{52}$$
$$R_2 = I(X; U|V) + \epsilon, \tag{53}$$
$$R_3 = I(X; U|V) - I(Y; U|V) + 2\epsilon. \tag{54}$$
2) **Encoding:** Upon observing a sequence X^n, Alice looks into the generated codebook trying to find a V^n that is jointly P_{VX}-typical with X^n. After selecting V^n, Alice looks into those sequences U^n that are generated by V^n, trying to find a U^n that is jointly P_{UVX}-typical with (V^n, X^n). During this process, if there are more than one such V^n or U^n, she randomly picks one such sequence; if there is no such sequence, she declares an error. If Alice finds such V^n and U^n, she sends the bin indices, M' and M'', of V^n and U^n to the fusion center.
3) **Decoding:** After receiving (M', M''), the fusion center first looks into $b(M')$ trying to find a unique $\hat{V}^n$ that is jointly P_{VY}-typical with Y^n. Then, it looks into $b_{\hat{V}^n}(M'')$ trying to find a unique $\hat{U}^n$ that is jointly P_{VUY}-typical with $(\hat{V}^n, Y^n)$. If there are more than one or no such sequence $\hat{V}^n(\hat{U}^n)$, it randomly selects a $\hat{U}^n$ as the decoded sequence.
4) **Function computing:** The fusion center computes the estimated value $\hat{\mathbf{f}} := \{g(\hat{U}_i, Y_i)\}_{i=1}^n$.
5) **Error analysis:** According to Lemma 1, the fusion center can correctly compute $\mathbf{f}$ as long as U^n is jointly typical with X^n and $\hat{U}^n = U^n$. Thus, the error is upper bounded by
$$\Pr\{\hat{V}^n \neq V^n|\mathcal{C}\} + \Pr\{\hat{U}^n \neq U^n|V^n, \mathcal{C}\}. \tag{55}$$
$\Pr\{\hat{V}^n \neq V^n|\mathcal{C}\}$ is upper bounded by the probabilities of the following two events: *Event-1: no jointly typical sequence V^n with X^n is found* (if V^n is jointly typical

with X^n, it will be jointly typical with Y^n since $V \to X \to Y$); *Event-2: there is a sequence other than* V^n *in* $b(M')$ *jointly typical with* Y^n. Since there are $2^{n(I(V;X)+\epsilon)}$ sequences V^n in $\mathcal{C}$, we can easily have that there exists an $\epsilon_1 \to 0$ (when n goes to infinity) so that

$$\Pr\{\text{Event-1}\} \le \epsilon_1. \tag{56}$$

Next, we will show that there also exists an $\epsilon_2 \to 0$ so that

$$\Pr\{\text{Event-2}\} \le \epsilon_2. \tag{57}$$

To show (57), it suffices to prove that there exists an $\epsilon' \to 0$ so that $|b(M')| \le 2^{n(I(V;Y)-\epsilon')}$. First, we have

$$\mathbb{E}[|b(M')|] = 2^{nR_0} \cdot \frac{1}{2^{R_1}} = 2^{n(I(Y;V)-\epsilon)}, \tag{58}$$

$$\begin{aligned}\mathrm{Var}(|b(M')|) &= 2^{nR_0} \cdot \frac{1}{2^{R_1}} \cdot (1 - \frac{1}{2^{R_1}}) \\ &\le 2^{n(I(Y;V)-\epsilon)}.\end{aligned} \tag{59}$$

Then, according to Chebyshev's inequality, we have

$$\begin{aligned}&\Pr\left\{\Big||b(M')| - \mathbb{E}[|b(M')|]\Big| \ge \frac{1}{2}\mathbb{E}[|b(M')|]\right\} \\ &\qquad \le \frac{\mathrm{Var}(|b(M')|)}{(\frac{1}{2}\mathbb{E}[|b(M')|])^2} \le \frac{4}{2^{n(I(Y;V)-\epsilon)}}.\end{aligned} \tag{60}$$

Thus, with high probability, we have that

$$\begin{aligned}|b(M')| &\in [\frac{1}{2} \cdot 2^{n(I(Y;V)-\epsilon)}, \frac{3}{2} \cdot 2^{n(I(Y;V)-\epsilon)}] \\ &:= [2^{n(I(Y;V)-\epsilon_1')}, 2^{n(I(Y;V)-\epsilon_2')}].\end{aligned} \tag{61}$$

We can conclude that (57) is true if we set $\epsilon' = \epsilon_2'$, and that

$$\Pr\{\hat{V}^n \ne V^n|\mathcal{C}\} \le \epsilon_1 + \epsilon_2. \tag{62}$$

Once V^n is correctly decoded, we can go further to upper bound the second term of (55). Similarly, $\Pr\{\hat{U}^n \ne U^n|V^n, \mathcal{C}\}$ is upper bounded by the probabilities of the following two events: *Event-3: no jointly typical sequence* U^n *with* (V^n, X^n) *is found*; *Event-4: there is a sequence other than* U^n *in* $b_{V^n}(M'')$ *jointly typical with* (V^n, Y^n). Since there are $2^{n(I(U;X|V)+\epsilon)}$ sequences U^n in $b_{V^n}(M'')$, we have, according to the Covering lemma [39, Lemma 3.3], that there exists an $\epsilon_3 \to 0$ so that

$$\Pr\{\text{Event-3}\} \le \epsilon_3. \tag{63}$$

Next, we will show that there also exists an $\epsilon_4 \to 0$ so that

$$\Pr\{\text{Event-4}\} \le \epsilon_4. \tag{64}$$

To show (64), we will apply the Packing lemma [39, Lemma 3.1] which suffices to prove that there exists an $\epsilon'' \to 0$ so that $|b_{V^n}(M'')| \le 2^{n(I(U;Y|V)-\epsilon'')}$: the procedure is similar as those steps upper bounding $|b(M')|$, thus omitted.

Hence, the total error probability is upper bounded by $\epsilon_1+\epsilon_2+\epsilon_3+\epsilon_4$, which goes to zero as n goes to infinity.

6) **Message rate**: The transmitted messages are (M', M''), thus, the rate is $I(X;V) - I(Y;V) + 2\epsilon + I(X;U|V) - I(Y;U|V) + 2\epsilon = I(X;U) - I(Y;U) + 4\epsilon$.
7) **Privacy leakage:** First, we have

$$\begin{aligned}&I(X^n; M', M''|Y^n, \mathcal{C}) \\ &\le H(M', M''|\mathcal{C}) \\ &\le H(M'|\mathcal{C}) + H(M''|\mathcal{C}) \\ &= n[I(X;V) - I(Y;V) + I(X;U|V) \\ &\qquad - I(Y;U|V) + 2\epsilon] \\ &= nI(X;U|Y) + 2n\epsilon.\end{aligned} \tag{65}$$

Before proceeding, we need the following two lemmas whose proofs are presented in Appendix A.

Lemma 3. *Given arbitrary* $\epsilon > 0$*, we have*

$$\liminf_{n\to\infty} \frac{1}{n} H(X^n|U^n, V^n, Z^n, \mathcal{C}) \ge H(X|U, Z) - \epsilon. \tag{66}$$

Lemma 4. *Given arbitrary* $\epsilon > 0$*, we have*

$$\begin{aligned}\liminf_{n\to\infty} \frac{1}{n} H(U^n|V^n, Z^n, \mathcal{C}) &\ge I(X;U|V) \\ &\quad - I(Z;U|V) - \epsilon.\end{aligned} \tag{67}$$

Now we bound $I(X^n; M', M'', Z^n|\mathcal{C})$ as follows

$$\begin{aligned}&I(X^n; M', M'', Z^n|\mathcal{C}) \\ &\le I(X^n; V^n, M'', Z^n|\mathcal{C}) \\ &= H(X^n|\mathcal{C}) - H(X^n|V^n, M'', Z^n, \mathcal{C}) \\ &= nH(X) - H(X^n, U^n|V^n, M'', Z^n, \mathcal{C}) \\ &\qquad + H(U^n|X^n, V^n, M'', Z^n, \mathcal{C}) \\ &\overset{(a)}{\le} nH(X) - H(X^n, U^n|V^n, M'', Z^n, \mathcal{C}) + n\epsilon \\ &= nH(X) - H(U^n|V^n, Z^n, M'', \mathcal{C}) \\ &\qquad - H(X^n|Z^n, U^n, V^n, M'', \mathcal{C}) + n\epsilon \\ &= nH(X) - H(U^n|V^n, Z^n, M'', \mathcal{C}) \\ &\qquad - H(X^n|Z^n, U^n, V^n, \mathcal{C}) + n\epsilon \\ &\overset{(c)}{\le} nI(X;Z,U) - H(U^n|V^n, Z^n, M'', \mathcal{C}) + 2n\epsilon \\ &= nI(X;Z,U) - H(U^n|V^n, Z^n, \mathcal{C}) \\ &\qquad + I(U^n; M''|V^n, Z^n, \mathcal{C}) + 2n\epsilon,\end{aligned} \tag{68}$$

where step (a) is true due to the fact that given V^n and M'', there are $2^{n(I(Y;U|V)-\epsilon)}$ sequences U^n in $b_{V^n}(M'')$, and the probability that there exists another $\bar{U}^n$ that is jointly typical with (X^n, V^n) is upper bounded by $2^{-n(I(X;U|V)-I(Y;U|V))} < \epsilon$, thus, it is easy to have

$$H(U^n|V^n, Z^n, M'', \mathcal{C}) \le n\epsilon. \tag{69}$$

And step (c) follows from Lemma 3. According to Lemma 4 , we have

$$H(U^n|V^n, Z^n, \mathcal{C}) \ge n(I(X;U|V) - I(Z;U|V)) - \epsilon. \tag{70}$$

On the other hand, we have that

$$\begin{aligned}&I(U^n; M''|V^n, Z^n, \mathcal{C}) \\ &= H(M''|V^n, Z^n, \mathcal{C}) - H(M''|U^n, V^n, Z^n, \mathcal{C}) \\ &\le H(M''|\mathcal{C}) \\ &= nI(X;U|V) - nI(Y;U|V) + 2n\epsilon.\end{aligned} \tag{71}$$

Thus, we have that

$$\frac{1}{n}I(X^n; M', M'', Z^n|\mathcal{C}) \leq I(X; Z, U) - [I(Y; U|V) - I(Z; U|V)] + 5\epsilon, \quad (72)$$

which indicates that $\frac{1}{n}H(X^n|M', M'', Z^n, \mathcal{C}) \geq H(X; Z, U) + [I(Y; U|V) - I(Z; U|V)] - 5\epsilon$.

Hence, the achievability proof is complete.

Converse:

It is equivalent to show that any achievable tuple (R, Δ_1, Δ_2) is contained in $\mathcal{S}$, i.e. there exists some admissible U w.r.t. X, Y and f, as well as a random variable V, such that (7), (8), (9) and (10) hold.

First of all, we have that

$$\begin{aligned} nR &\geq H(M) - n\epsilon \\ &\geq H(M|Y^n) - n\epsilon \\ &\geq H(M|Y^n) - H(M|X^n) - n\epsilon \\ &= I(M; X^n) - I(M; Y^n) - n\epsilon \\ &= \sum_{i=1}^{n} I(M; X_i|X^{i-1}, Y_{i+1}^n) - I(M; Y_i|X^{i-1}, Y_{i+1}^n) - n\epsilon \\ &= \sum_{i=1}^{n} [I(M, X^{i-1}, Y_{i+1}^n; X_i) - I(M, X^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon. \end{aligned} \quad (73)$$

On the other hand, the following Markov chains are true,

$$X_i \to (M, X^{i-1}, Y_{i+1}^n) \to Z^{i-1}, \quad (74)$$

$$Y_i \to (M, X^{i-1}, Y_{i+1}^n) \to Z^{i-1}, \quad (75)$$

which are implied by

$$\begin{aligned} &(Y_i^n, X^n) \to X^{i-1} \to Z^{i-1} \\ \Rightarrow\ &(M, X_i, Y_i^n) \to X^{i-1} \to Z^{i-1} \\ \Rightarrow\ &(X_i, Y_i) \to (M, X^{i-1}, Y_{i+1}^n) \to Z^{i-1}. \end{aligned} \quad (76)$$

Thus, it follows that

$$\begin{aligned} nR &\geq \sum_{i=1}^{n} [I(M, X^{i-1}, Y_{i+1}^n; X_i) - I(M, X^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon \quad (77) \\ &= \sum_{i=1}^{n} [I(M, X^{i-1}, Y_{i+1}^n, Z^{i-1}; X_i) - I(M, X^{i-1}, Y_{i+1}^n, Z^{i-1}; Y_i)] - n\epsilon \\ &= \sum_{i=1}^{n} [I(U_i; X_i) - I(U_i; Y_i)] - n\epsilon \\ &= n[I(U; X) - I(U; Y)] - n\epsilon, \quad (78) \end{aligned}$$

in which U_i and U are defined by $U_i := (M, X^{i-1}, Y_{i+1}^n, Z^{i-1})$ and $U := (U_J, J)$, J is an independent random variable uniformly distributed over $[1 : n]$. And we can easily verify that $U \to X \to Y$ holds.

Furthermore, according to Fano's inequality, we have

$$\begin{aligned} n\epsilon &\geq H(\mathbf{f}|\hat{\mathbf{f}}) \\ &\geq H(f^n|\hat{\mathbf{f}}, M, Y^n) \\ &= H(f^n|M, Y^n) \\ &= \sum_{i=1}^{n} H(f_i|f^{i-1}, M, Y^n) \\ &\geq \sum_{i=1}^{n} H(f_i|f^{i-1}, M, Y^n, X^{i-1}) \\ &\overset{(a)}{=} \sum_{i=1}^{n} H(f_i|M, Y^n, X^{i-1}) \\ &\overset{(b)}{=} \sum_{i=1}^{n} H(f_i|Y_i, M, Y_{i+1}^n, X^{i-1}) \\ &\geq \sum_{i=1}^{n} H(f_i|Y_i, M, Y_{i+1}^n, X^{i-1}) \\ &\geq \sum_{i=1}^{n} H(f_i|Y_i, M, Y_{i+1}^n, X^{i-1}, Z^{i-1}) \\ &= \sum_{i=1}^{n} H(f_i|Y_i, U_i) \\ &= nH(f|Y, U), \end{aligned} \quad (79)$$

where step (a) is true since f^{i-1} is a function of (X^{i-1}, Y^{i-1}), and step (b) follows from the Markov chain $f_i \to (Y_i, Y_{i+1}^n, X^{i-1}, M) \to Y^{i-1}$, which is indicated by

$$\begin{aligned} &(X^n, Y_i^n) \to X^{i-1} \to Y^{i-1} \\ \Rightarrow\ &(M, X_i, Y_i^n) \to X^{i-1} \to Y^{i-1} \\ \overset{(a)}{\Rightarrow}\ &(X_i, Y_i) \to (M, Y_{i+1}^n, X^{i-1}) \to Y^{i-1}. \end{aligned} \quad (80)$$

Here (a) is true due to the weak union property of the Markov chain [41]. Thus, $H(f|Y, U) \leq \epsilon$. In addition, as ϵ can be made arbitrarily small, we can claim that this constructed random variable U is admissible w.r.t. X, Y and f.

In addition, as (76) implies that the following Markov chain holds

$$X_i \to (Y_i, M, X^{i-1}, Y_{i+1}^n) \to Z^{i-1}, \quad (81)$$

it follows that

$$\begin{aligned} n\Delta_1 &\geq I(X^n; M|Y^n) - n\epsilon \quad (82) \\ &= H(X^n|Y^n) - H(X^n|M, Y^n) - n\epsilon \\ &= nH(X|Y) - H(X^n|M, Y^n) - n\epsilon \\ &= nH(X|Y) - \sum_{i=1}^{n} H(X_i|M, Y^n, X^{i-1}) - n\epsilon \\ &\geq nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, M, Y_{i+1}^n, X^{i-1}) - n\epsilon \\ &= nH(X|Y) - \sum_{i=1}^{n} H(X_i|Y_i, M, Y_{i+1}^n, X^{i-1}, Z^{i-1}) - n\epsilon \\ &= nH(X|Y) - nH(X|Y, U) - n\epsilon \\ &= nI(X; U|Y) - n\epsilon. \quad (83) \end{aligned}$$

As the final step, we now show (10). It follows that

$$\begin{aligned}
&I(X^n; M, Z^n)\\
&= I(M; X^n) + I(X^n; Z^n|M)\\
&= I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n)\\
&\qquad + I(M; Z^n) + I(X^n; Z^n|M)\\
&= I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n)\\
&\qquad + I(M, X^n; Z^n)\\
&= I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n)\\
&\qquad + I(X^n; Z^n)\\
&= I(M; X^n) - I(M; Y^n) + I(M; Y^n) - I(M; Z^n)\\
&\qquad + nI(X; Z). \qquad (84)
\end{aligned}$$

In the right-hand side of (84), we have

$$\begin{aligned}
&I(M; X^n) - I(M; Y^n)\\
&= \sum_{i=1}^{n} [I(M; X_i|X^{i-1}, Y_{i+1}^n) - I(M; Y_i|X^{i-1}, Y_{i+1}^n)]\\
&= \sum_{i=1}^{n} [I(M, X^{i-1}, Y_{i+1}^n; X_i) - I(M, X^{i-1}, Y_{i+1}^n; Y_i)]\\
&= \sum_{i=1}^{n} [I(M, X^{i-1}, Y_{i+1}^n, Z^{i-1}; X_i)\\
&\qquad - I(M, X^{i-1}, Y_{i+1}^n, Z^{i-1}; Y_i)]\\
&= n[I(U; X) - I(U; Y)], \qquad (85)
\end{aligned}$$

and

$$\begin{aligned}
&I(M; Y^n) - I(M; Z^n)\\
&= \sum_{i=1}^{n} [I(M; Y_i|Z^{i-1}, Y_{i+1}^n) - I(M; Z_i|Z^{i-1}, Y_{i+1}^n)]\\
&= \sum_{i=1}^{n} [I(M, Z^{i-1}, Y_{i+1}^n; Y_i) - I(M, Z^{i-1}, Y_{i+1}^n; Z_i)]\\
&= \sum_{i=1}^{n} [I(V_i; Y_i) - I(V_i; Z_i)]\\
&= n[I(V; Y) - I(V; Z)], \qquad (86)
\end{aligned}$$

in which $V_i := (M, Y_{i+1}^n, Z^{i-1})$ and $V := (V_J, J)$, J is an independent random variable uniformly distributed over $[1 : n]$. For this construction of V, we can conclude that $V \to U \to X \to (Y, Z)$ is true. Thus, it follows that

$$\begin{aligned}
&\frac{1}{n} I(X^n; M, Z^n)\\
&= I(U; X) - I(U; Y) + I(V; Y) - I(V; Z) + I(X; Z)\\
&= I(U; X) - I(U; Y|V) - I(V; Z) + I(X; Z)\\
&= I(U; X) - I(U; Y|V) + I(X; Z|V)\\
&= I(U; X) - I(U; Y|V) + I(U, X; Z|V)\\
&= I(U; X) - I(U; Y|V) + I(U; Z|V) + I(X; Z|U, V)\\
&= I(U; X) - I(U; Y|V) + I(U; Z|V) + I(X; Z|U)\\
&= I(X; U, Z) - I(U; Y|V) + I(U; Z|V)\\
&\geq I(X; U, Z) - [I(U; Y|V) - I(U; Z|V)]^+, \qquad (87)
\end{aligned}$$

which implies that

$$\begin{aligned}
\Delta_2 &\leq \frac{1}{n} H(X^n|M, Z^n) + \epsilon\\
&= \frac{1}{n} (H(X^n) - I(X^n; M, Z^n)) + \epsilon\\
&\leq H(X) - I(X; U, Z) + [I(U; Y|V) - I(U; Z|V)]^+ + \epsilon\\
&= H(X|U, Z) + [I(U; Y|V) - I(U; Z|V)]^+ + \epsilon. \qquad (88)
\end{aligned}$$

Hence, the converse is complete.

The proof of bounding the cardinality of the valuable U is lengthy and the derivation procedure follows the Cardinality Bounding Techniques in [39, Appendix C], thus is omitted in the paper.

B. Proof of Theorem 2

Converse:

In this part, we show that any achievable tuple $(R, D, \Delta_1, \Delta_2)$ is contained in the region defined by (21)-(25).

First, according to (3), we have that

$$\begin{aligned}
&nR\\
&\geq H(M) - \epsilon\\
&\geq I(M; X^n) - I(M; Y^n) - \epsilon\\
&= \sum_{i=1}^{n} \Big[I(M; X_i|X^{i-1}, Y_{i+1}^n) - I(M; Y_i|X^{i-1}, Y_{i+1}^n) \Big] - \epsilon\\
&= \sum_{i=1}^{n} \Big[I(M, X^{i-1}, Y_{i+1}^n; X_i) - I(M, X^{i-1}, Y_{i+1}^n; Y_i) \Big] - \epsilon\\
&\overset{(a)}{=} \sum_{i=1}^{n} \Big[I(M, X^{i-1}, Y_{i+1}^n, Y^{i-1}, Z^{i-1}; X_i)\\
&\qquad - I(M, X^{i-1}, Y_{i+1}^n, Y^{i-1}, Z^{i-1}; Y_i) \Big] - \epsilon\\
&= \sum_{i=1}^{n} [I(U_i; X_i) - I(U_i; Y_i)] - \epsilon\\
&= n\,[I(U; X) - I(U; Y)] - \epsilon, \qquad (89)
\end{aligned}$$

where step (a) follows from the following Markov chain

$$(X_i, Y_i) \to (M, X^{i-1}, Y_{i+1}^n) \to (Y^{i-1}, Z^{i-1}), \qquad (90)$$

which is implied by the following Markov chain

$$(X^n, Y_i^n) \to (X^{i-1}) \to (Y^{i-1}, Z^{i-1}). \qquad (91)$$

And $U := (U_J, J)$ with J uniformly distributed in $[1 : n]$, and U_i is defined as

$$U_i := (M, X^{i-1}, Y_{i+1}^n, Y^{i-1}, Z^{i-1}), \qquad (92)$$

and we have $U_i \to X_i \to (Y_i, Z_i)$, which follows from

$$\begin{aligned}
&(X^n, Y^{i-1}, Y_{i+1}^n, Z^{i-1}) \to X_i \to (Y_i, Z_i)\\
\Rightarrow\ &(M, X^{i-1}, Y_{i+1}^n, Y^{i-1}, Z^{i-1}) \to X_i \to (Y_i, Z_i). \qquad (93)
\end{aligned}$$

Second, it follows from (2) that

$$\begin{aligned}
D &\geq \frac{1}{n}E\left[d(\mathbf{f}(X^n,Y^n),\hat{\mathbf{f}}(M,Y^n))\right]-\epsilon\\
&=\frac{1}{n}E\left[\sum_{i=1}^{n}d(f(X_i,Y_i),\hat{f}_i(M,Y^n))\right]-\epsilon\\
&\overset{(a)}{\geq}\frac{1}{n}E\left[\sum_{i=1}^{n}d(f(X_i,Y_i),g(M,Y^n,X^{i-1},Z^{i-1},i))\right]-\epsilon\\
&=\frac{1}{n}E\left[\sum_{i=1}^{n}d(f(X_i,Y_i),g(U_i,i,Y_i))\right]-\epsilon\\
&=E\left[\sum_{i=1}^{n}\frac{1}{n}d(f(X_i,Y_i),g(U_i,i,Y_i))\right]-\epsilon\\
&=E\left[d(f(X,Y),g(U,Y_I))\right]-\epsilon\\
&=E\left[d(f(X,Y),g(U,Y))\right]-\epsilon, \qquad (94)
\end{aligned}$$

where step (a) holds as $\hat{f}_i(M,Y^n)$ is a function of M and Y^n in general, hence there must exist some function, say g, such that the distortion decreases since more information is provided for each $i\in[1:n]$.

In addition, we have

$$\begin{aligned}
n\Delta_1 &\geq I(X^n;M|Y^n)-n\epsilon\\
&=H(X^n|Y^n)-H(X^n|M,Y^n)-n\epsilon\\
&=nH(X|Y)-\sum_{i=1}^{n}H(X_i|M,Y^n,X^{i-1})-n\epsilon\\
&\overset{(a)}{=}nH(X|Y)-\sum_{i=1}^{n}H(X_i|M,Y^n,X^{i-1},Z^{i-1})-2n\epsilon\\
&=nH(X|Y)-\sum_{i=1}^{n}H(X_i|Y_i,U_i)-n\epsilon\\
&=nH(X|Y)-nH(X|Y,U)-n\epsilon\\
&=nI(X;U|Y)-n\epsilon, \qquad (95)
\end{aligned}$$

in which step (a) is true due to the following Markov chain

$$X_i\rightarrow(M,Y^n,X^{i-1})\rightarrow Z^{i-1}. \qquad (96)$$

This Markov chain is implied by (90) due to the decomposition property of Markov chain [41].

As the final step, the derivation is similar as the procedure from (84) to (88).

First, we have

$$\begin{aligned}
&I(X^n;M,Z^n)\\
&=I(M;X^n)-I(M;Y^n)+I(M;Y^n)-I(M;Z^n)\\
&\qquad+nI(X;Z). \qquad (97)
\end{aligned}$$

Furthermore, it follows from (89) that

$$I(M;X^n)-I(M;Y^n)=n[I(U;X)-I(U;Y)], \qquad (98)$$

while

$$\begin{aligned}
&I(M;Y^n)-I(M;Z^n)\\
&=\sum_{i=1}^{n}[I(M;Y_i|Z^{i-1},Y_{i+1}^n)-I(M;Z_i|Z^{i-1},Y_{i+1}^n)]\\
&=\sum_{i=1}^{n}[I(V_i;Y_i)-I(V_i;Z_i)]\\
&=n[I(V;Y)-I(V;Z)], \qquad (99)
\end{aligned}$$

with $V_i:=(M,Y_{i+1}^n,Z^{i-1})$ and $V:=(V_J,J)$, J is an independent random variable uniformly distributed over $[1:n]$. Based on the definition of U and V stated above, we have the Markov chain relationship: $V\rightarrow U\rightarrow X\rightarrow(Y,Z)$ according to (93). Combine (97)-(99), and we have

$$\begin{aligned}
&I(X^n;M,Z^n)\\
&=I(U;X)-I(U;Y)+I(V;Y)-I(V;Z)+I(X;Z)\\
&=I(X;U,Z)-I(U;Y|V)+I(U;Z|V)\\
&\geq I(X;U,Z)-[I(U;Y|V)-I(U;Z|V)]^+. \qquad (100)
\end{aligned}$$

Finally, we obtain

$$\begin{aligned}
\Delta_2 &\leq \frac{1}{n}H(X^n|M,Z^n)+\epsilon\\
&=\frac{1}{n}(H(X^n)-I(X^n;M,Z^n))+\epsilon\\
&\leq H(X)-I(X;U,Z)+[I(U;Y|V)-I(U;Z|V)]^+\epsilon\\
&=H(X|U,Z)+[I(U;Y|V)-I(U;Z|V)]^+\epsilon. \qquad (101)
\end{aligned}$$

Hence, the converse proof is complete.

Achievability:

To prove the achievability for Theorem 2, we use the same achievability scheme as stated in the proof for Theorem 1. The only difference is the range of PMF $P_{XYZ}P_{U|X}P_{V|U}$. In this scheme, $P_{XYZ}P_{U|X}P_{V|U}$ is given, subject to that there exists a function g of (U,Y) achieving $E(d(f(X,Y),g(U,Y)))\leq D+\epsilon$ and the function g is fixed for function computation. Once $P_{XYZ}P_{U|X}P_{V|U}$ and g is fixed, we can follow the same procedures in the proof of Theorem 1 to obtain the desired result.

C. Proof of Theorem 3

Converse:

In the following, we define

$$U_{1i}:=(M_1,X_1^{i-1},Z^{i-1},Y_{i+1}^n), \qquad (102)$$

$$V_{1i}:=(M_1,Z^{i-1},Y_{i+1}^n), \qquad (103)$$

$$U_{2i}:=(M_2,X_2^{i-1},Z^{i-1},Y_{i+1}^n), \qquad (104)$$

$$V_{2i}:=(M_2,Z^{i-1},Y_{i+1}^n). \qquad (105)$$

Furthermore, define $U_1:=(U_{1J},J)$ with J being a random variable independent with all other random variables and uniformly distributed over $[1:n]$. Define V_1, U_2 and V_2 in the same manner. We can verify that the Markov chain $V_1\rightarrow U_1\rightarrow X_1\rightarrow(X_2,Y,Z)$ holds, as we have

$$\begin{aligned}
&(X_1^n,Z^{i-1},Y_{i+1}^n)\rightarrow X_{1i}\rightarrow(X_{2i},Y_i,Z_i)\\
\Rightarrow\quad &(M_1,X_1^{i-1},Z^{i-1},Y_{i+1}^n)\rightarrow X_{1i}\rightarrow(X_{2i},Y_i,Z_i). \qquad (106)
\end{aligned}$$

Similarly, we can verify that $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$ holds.

In the following, we show (33)-(38) one by one. First, we have

$$\begin{aligned}
nR_1 &\geq H(M_1) - n\epsilon \\
&\geq I(M_1; X_1^n) - I(M_1; Y^n) - n\epsilon \\
&= \sum_{i=1}^{n}[I(M_1; X_{1i}|X_1^{i-1}, Y_{i+1}^n) \\
&\qquad - I(M_1; Y_i|X_1^{i-1}, Y_{i+1}^n)] - n\epsilon \\
&= \sum_{i=1}^{n}[I(M_1, X_1^{i-1}, Y_{i+1}^n; X_{1i}) \\
&\qquad - I(M_1, X_1^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon \\
&\overset{(a)}{=} \sum_{i=1}^{n}[I(M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n; X_{1i}) \\
&\qquad - I(M_1, X_1^{i-1}, Z^{i-1}, Y_{i+1}^n; Y_i)] - n\epsilon \\
&= \sum_{i=1}^{n}[I(U_{1i}; X_{1i}) - I(U_{1i}; Y_i)] - n\epsilon \\
&= n[I(U_1; X_1) - I(U_1; Y)] - n\epsilon \\
&= nI(U_1; X_1|Y) - n\epsilon \\
&= n[I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1)] - n\epsilon, \\
&= n[I(V_1; X_1, V_2|Y) - I(V_1; V_2|Y, X_1)] - n\epsilon \\
&\quad + n[I(U_1; X_1, U_2|Y, V_1) - I(U_1; U_2|X_1, Y, V_1)], \\
&\geq n[I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1) \\
&\quad - I(V_1; V_2|Y, X_1) - I(U_1; U_2|X_1, Y, V_1)] - n\epsilon, \quad (107)
\end{aligned}$$

where step (a) follows a similar Markov chain relationship as derived in (76). Thus, we have

$$\begin{aligned}
R_1 &\geq I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1) \\
&\quad - I(V_1; V_2|Y, X_1) - I(U_1; U_2|X_1, Y, V_1) - \epsilon. \quad (108)
\end{aligned}$$

Similarly, we have

$$\begin{aligned}
R_2 &\geq I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) \\
&\quad + I(V_1; V_2|Y, X_2) + I(U_1; U_2|X_2, Y, V_2) - \epsilon. \quad (109)
\end{aligned}$$

In addition, it follows that

$$\begin{aligned}
R_1 + R_2 &\geq \frac{1}{n}H(M_1) - \epsilon + \frac{1}{n}H(M_2) - \epsilon \\
&\geq \frac{1}{n}H(M_1, M_2) - 2\epsilon \\
&\geq \frac{1}{n}I(M_1, M_2; X_1^n, X_2^n) - \frac{1}{n}I(M_1, M_2; Y^n) - 2\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1, M_2; X_{1i}, X_{2i}|X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n) \\
&\quad - I(M_1, M_2; Y_i|X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n)] - 2\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n; X_{1i}, X_{2i}) \\
&\quad - I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n; Y_i)] - 2\epsilon \\
&= \frac{1}{n}\sum_{i=1}^{n}[I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Z^{i-1}, Y_{i+1}^n; X_{1i}, X_{2i}) \\
&\quad - I(M_1, M_2, X_1^{i-1}, X_2^{i-1}, Z^{i-1}, Y_{i+1}^n; Y_i)] - 2\epsilon \\
&= I(U_1, U_2; X_1, X_2) - I(U_1, U_2; Y) - 2\epsilon \\
&= I(U_1, U_2; X_1, X_2|Y) - 2\epsilon \\
&= I(U_1, U_2; X_1, X_2|Y, V_1, V_2) + I(V_1, V_2; X_1, X_2|Y) - 2\epsilon \\
&= I(V_1; X_1, X_2|Y) + I(V_2; X_1, X_2|Y, V_1) - 2\epsilon \\
&\quad + I(U_1; X_1, X_2|Y, V_1, V_2) + I(U_2; X_1, X_2|Y, U_1, V_2) \\
&\geq I(V_1; X_1|Y) + I(V_2; X_2|Y, V_1) + I(U_1; X_1|Y, V_1, V_2) \\
&\quad + I(U_2; X_2|Y, U_1, V_2) - 2\epsilon. \quad (110)
\end{aligned}$$

Furthermore, we have

$$\begin{aligned}
n\Delta_1 &\geq I(X_1^n, X_2^n; M_1, M_2|Y^n) - n\epsilon \\
&= H(X_1^n, X_2^n|Y^n) - H(X_1^n, X_2^n|M_1, M_2, Y^n) - n\epsilon \\
&= nH(X_1, X_2|Y) - H(X_1^n, X_2^n|M_1, M_2, Y^n) - n\epsilon \\
&= nH(X_1, X_2|Y) - \sum_{i=1}^{n} H\Big(X_{1i}, X_{2i}\Big| \\
&\qquad M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}\Big) - n\epsilon \\
&\overset{(a)}{=} nH(X_1, X_2|Y) - \sum_{i=1}^{n} H\Big(X_{1i}, X_{2i}\Big| \\
&\qquad M_1, M_2, Y_{i+1}^n, Z^{i-1}, X_1^{i-1}, X_2^{i-1}\Big) - n\epsilon \\
&= nH(X_1, X_2|Y) - \sum_{i=1}^{n} H(X_{1i}, X_{2i}\big| \\
&\qquad Y_i, U_{1i}, U_{2i}) - n\epsilon \\
&= nH(X_1, X_2|Y) - nH(X_1, X_2|Y, U_1, U_2) - n\epsilon \\
&= nI(X_1, X_2; U_1, U_2|Y) - n\epsilon, \quad (111)
\end{aligned}$$

in which step (a) is due to the following Markov chain:

$$\begin{aligned}
\big((X_1)_i, (X_2)_i\big) &\to \big(M_1, M_2, Y_{i+1}^n, X_1^{i-1}, X_2^{i-1}\big) \\
&\to \big(Y^{i-1}, Z^{i-1}\big). \quad (112)
\end{aligned}$$

This relationship is implied by

$$\begin{aligned}
\big((X_1)_i, (X_2)_i, M_1, M_2, Y_{i+1}^n\big) &\to \big(X_1^{i-1}, X_2^{i-1}\big) \\
&\to \big(Y^{i-1}, Z^{i-1}\big). \quad (113)
\end{aligned}$$

In addition, following similar steps from (84) to (88) by replacing X with (X_1, X_2), U with (U_1, U_2), V with (V_1, V_2) and M with (M_1, M_2), we can obtain

$$\begin{aligned}
\Delta_2 \leq H(X_1, X_2|U_1, U_2, Z) &+ \big[I(U_1, U_2; Y|V_1, V_2) \\
&- I(U_1, U_2; Z|V_1, V_2)\big]^+ + \epsilon. \quad (114)
\end{aligned}$$

As the last step, it follows that

$$\begin{aligned} n\epsilon &\geq H(f^n|M_1, M_2, Y^n) \\ &= \sum_{i=1}^{n} H(f_i|f^{i-1}, M_1, M_2, Y^n) \\ &\geq \sum_{i=1}^{n} H(f_i|f^{i-1}, M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\ &\geq \sum_{i=1}^{n} H(f_i|M_1, M_2, Y^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\ &= \sum_{i=1}^{n} H(f_i|M_1, M_2, Y_i^n, X_1^{i-1}, X_2^{i-1}, Z^{i-1}) \\ &= \sum_{i=1}^{n} H(f_i|Y_i, U_{1i}, U_{2i}) \\ &= nH(f|Y, U_1, U_2). \end{aligned} \tag{115}$$

Finally, the fact that ϵ is an arbitrarily small number completes the converse proof.

Achievability:

In this part, we show that given any $P_{U_1V_1U_2V_2X_1X_2YZ} = P_{X_1X_2YZ}P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$ with $H(f|U_1, U_2, Y) = 0$, any tuple $(R_1, R_2, \Delta_1, \Delta_2)$ satisfying the conditions from (33) to (38) is achievable. Since given $P_{U_1V_1U_2V_2X_1X_2YZ}$, the values of the right-hand side of (36) and (37) are fixed, it suffices to consider the corner point with

$$R_1 = I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1, V_2), \tag{116}$$

$$R_2 = I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2), \tag{117}$$

and the other corner point with

$$R_1 = I(V_1; X_1|Y, V_2) + I(U_1; X_1|Y, U_2, V_1), \tag{118}$$

$$R_2 = I(V_2; X_2|Y) + I(U_2; X_2|Y, V_1, V_2), \tag{119}$$

and at the corner points, we need to guarantee that $\Delta_1 \leq I(X_1, X_2; U_1, U_2|Y) + \epsilon$ and $\Delta_2 \geq H(X_1, X_2|U_1, U_2, Z) + [I(U_1, U_2; Y|V_1, V_2) - I(U_1, U_2; Z|V_1, V_2)]^+ - \epsilon$, for sufficiently small value $\epsilon > 0$. Due to the symmetry of the above two corner points, we only consider the former one.

1) **Codebook ($\mathcal{C}$) construction:**
   $\mathcal{C}_A$ *at Alice*. Given $P_{X_1X_2YZ}\ P_{U_1|X_1}P_{V_1|U_1}P_{U_2|X_2}P_{V_2|U_2}$, randomly and independently generate $2^{nR_{10}}$ sequences V_1^n according to $\prod_{i=1}^{n} P_{V_1}(v_{1i})$, and assign each V_1^n into $2^{nR_{11}}$ bins (indexed by M_{11}) using a uniform distribution. For each generated sequence V_1^n generate $2^{nR_{12}}$ sequences U_1^n according to $\prod_{i=1}^{n} P_{U_1|V_1}(u_{1i}|v_{1i})$ and assign each U_1^n into $2^{nR_{13}}$ sub-bins indexed by M_{12}, using a similar manner as above. In addition, we use $b_A(M_{11})$ and $b_A(M_{12}|V_1^n)$ to denote the corresponding bin and sub-bin indexed by M_{11} and M_{12} respectively, and set

$$R_{10} = I(V_1; X_1) + \epsilon, \tag{120}$$

$$R_{11} = I(V_1; X_1) - I(V_1; Y) + 2\epsilon, \tag{121}$$

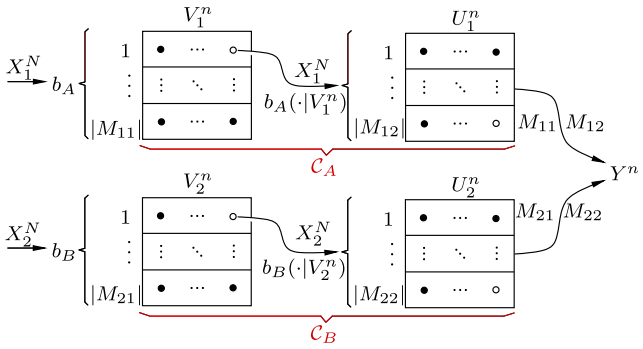

Fig. 4. Encoding scheme.

$$R_{12} = I(U_1; X_1|V_1) + \epsilon, \tag{122}$$

$$R_{13} = I(U_1; X_1|V_1) - I(U_1; Y, V_2|V_1) + 2\epsilon. \tag{123}$$

$\mathcal{C}_B$ *at Bob*. Similar to $\mathcal{C}_A$, generate $2^{nR_{20}}$ sequences V_2^n according to $\prod_{i=1}^{n} P_{V_2}(v_{2i})$, and assign these sequences into $2^{nR_{21}}$ bins indexed by M_{21}; For each V_2^n, generated $2^{nR_{22}}$ sequences U_2^n and assign each U_2^n into $2^{nR_{23}}$ sub-bins indexed by M_{22}. The bin and sub-bin are denoted by $b_B(M_{21})$ and $b_B(M_{22}|V_2^n)$, respectively, and set

$$R_{20} = I(V_2; X_2) + \epsilon, \tag{124}$$

$$R_{21} = I(V_2; X_2) - I(V_2; YV_1) + 2\epsilon, \tag{125}$$

$$R_{22} = I(U_2; X_2|V_2) + \epsilon, \tag{126}$$

$$R_{23} = I(U_2; X_2|V_2) - I(U_2; YU_1|V_2) + 2\epsilon. \tag{127}$$

2) **Encoding:** As shown in Fig. 4, upon observing a sequence X_1^n, Alice looks into $\mathcal{C}_A$ trying to find a V_1^n that is jointly $P_{V_1X_1}$-typical with X_1^n. After find the V_1^n, she looks into those sequences U_1^n generated by V_1^n, trying to find a U_1^n that is jointly $P_{V_1U_1X_1}$-typical with (V_1^n, X_1^n). In each step, if there are more than one desired sequence, she randomly picks one; Otherwise, she declares an error if no desired sequence is found. Then, Alice sends the bin index M_{11} of V_1^n and sub-bin index M_{12} of U_1^n to the fusion center.
   Similar to the encoding procedures of Alice's side, Bob looks into $\mathcal{C}_B$ to find a V_2^n and a U_2^n, and sends the indices M_{21} and M_{22} to the fusion center.
3) **Decoding:** After receiving messages M_{11}, M_{12}, M_{21} and M_{22}, the fusion center first looks into bin $b_A(M_{11})$, trying to find a unique $\hat{V}_1^n$ that is jointly P_{V_1Y}-typical with Y^n. If there are more than one such sequence or no such sequence, Bob randomly selects a $\hat{V}_1^n$ as the decoded sequence. Using the same decoding strategy within corresponding bins/sub-bins, it take turns to decode $\hat{V}_2^n$ with $(Y^n, \hat{V}_1^n)$, $\hat{U}_1^n$ with $(Y^n, \hat{V}_1^n, \hat{V}_2^n)$ and $\hat{U}_2^n$ with $(Y^n, \hat{U}_1^n, \hat{V}_2^n)$.
4) **Function computing:** The fusion center computes the estimated value $\hat{\mathbf{f}}$ based on $(\hat{U}_1^n, \hat{U}_2^n, Y^n)$.
5) **Error analysis:** Without much modification to Lemma 1, we can easily obtain that the fusion center can correctly compute $\mathbf{f}$ provided that U_1^n is jointly typical with X_1^n and U_2^n is jointly typical with X_2^n.

Thus, the error probability is upper bounded by the two events: 1). (U_1^n, X_1^n) or (U_2^n, X_2^n) are not jointly typical; 2). The fusion center cannot decode (U_1^n, U_2^n) correctly.

First of all, based on the parameters provided in this scheme, we can easily verify that with a high probability, there exists at least one pair (U_1^n, U_2^n) such that (U_1^n, X_1^n) and (U_2^n, X_2^n) are jointly typical respectively. Furthermore, we can easily obtain that the fusion center can correctly decode (U_1^n, U_2^n) with a high probability following the similar analysis in the achievability part in Theorem 1. Thus, the fusion center can correctly compute $\mathbf{f}$ with a high probability.

6) **Message rates:** From the above scheme, we have

$$\begin{aligned} R_1 &= R_{11} + R_{13} \\ &= I(V_1; X_1) - I(V_1; Y) + I(U_1; X_1|V_1) \\ &\qquad - I(U_1; Y, V_2|V_1) + 4\epsilon \\ &= I(V_1; X_1|Y) + I(U_1, X_1|Y, V_1, V_2) + 4\epsilon, \end{aligned} \tag{128}$$

and

$$\begin{aligned} R_2 &= R_{21} + R_{23} \\ &= I(V_2; X_2) - I(V_2; Y, V_1) + I(U_2; X_2|V_2) \\ &\qquad - I(U_2; Y, U_1|V_2) + 4\epsilon \\ &= I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) + 4\epsilon. \end{aligned} \tag{129}$$

7) **Privacy leakage:** First, it is easy to obtain that

$$\begin{aligned} &\frac{1}{n} I(X_1^n, X_2^n; M_{11}, M_{12}, M_{21}, M_{22}|Y^n, \mathcal{C}) \\ &\le H(M_{11}, M_{12}, M_{21}, M_{22}|\mathcal{C}) \\ &= I(V_1; X_1|Y) + I(U_1; X_1|Y, V_1, V_2) \\ &\qquad + I(V_2; X_2|Y, V_1) + I(U_2; X_2|Y, U_1, V_2) + 8\epsilon \\ &= I(V_1, V_2; X_1, X_2|Y) + I(U_1, U_2; X_1, X_2|Y, V_1, V_2) + 8\epsilon \\ &= I(X_1, X_2; U_1, U_2|Y) + 8\epsilon. \end{aligned} \tag{130}$$

Furthermore, we have

$$\begin{aligned} &H(X_1^n, X_2^n|M_{11}, M_{12}, M_{21}, M_{22}, Z^n, \mathcal{C}) \\ &\ge H(X_1^n, X_2^n|V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) \\ &\ge H(X_1^n, X_2^n, U_1^n, U_2^n|V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) - n\epsilon \\ &= H(U_1^n, U_2^n|V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) \\ &\quad + H(X_1^n, X_2^n|U_1^n, U_2^n, V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) - n\epsilon \\ &= H(U_1^n, U_2^n|V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) \\ &\quad + H(X_1^n, X_2^n|U_1^n, U_2^n, V_1^n, V_2^n, Z^n, \mathcal{C}) - n\epsilon \\ &\overset{(a)}{\ge} H(U_1^n, U_2^n|V_1^n, V_2^n, M_{12}, M_{22}, Z^n, \mathcal{C}) \\ &\quad + nH(X_1, X_2|U_1, U_2, Z) - 2n\epsilon \\ &= nH(X_1, X_2|U_1, U_2, Z) + H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C}) \\ &\quad - I(U_1^n, U_2^n; M_{12}, M_{22}|V_1^n, V_2^n, Z^n, \mathcal{C}) - 2n\epsilon \\ &\ge nH(X_1, X_2|U_1, U_2, Z) + H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C}) \\ &\quad - H(M_{12}, M_{22}) - 2n\epsilon, \end{aligned} \tag{131}$$

where step (a) can be easily verified following similar arguments as those in the proof of Lemma 3.

Now, we bound each term above. First, we have

$$\begin{aligned} &\frac{1}{n} H(M_{21}, M_{22}) \le R_{13} + R_{23} \\ &= I(U_1; X_1|V_1) - I(U_1; Y, V_2|V_1) \\ &\qquad + I(U_2; X_2|V_2) - I(U_2; Y, U_1|V_2) + 4\epsilon \\ &= I(U_1; X_1|Y, V_1, V_2) + I(U_2; X_2|Y, U_1, V_2) + 4\epsilon \\ &= I(U_1, U_2; X_1, X_2|Y, V_1, V_2) + 4\epsilon. \end{aligned} \tag{132}$$

We bound the term $H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C})$ as follows. Given V_1^n, there are $2^{nR_{12}}$ sequences U_1^n that are generated by V_1^n, and the probability of that each U_1^n is jointly typical with (V_1^n, V_2^n, Z^n) is around $2^{-nI(U_1; V_2, Z|V_1)}$. Thus, there are around $2^{n(I(U_1; X_1|V_1) - I(U_1; V_2, Z|V_1))}$ sequences U_1^n that is jointly typical with (V_1^n, V_2^n, Z^n). Similarly, for each such U_1^n, there are around $2^{n(I(U_2; X_2|V_2) - I(U_2; U_1, Z|V_2) + \epsilon)}$ sequences U_2^n that are generated by V_2^n and jointly typical with $(U_1^n, V_1^n, V_2^n, Z^n)$. Hence, given (V_1^n, V_2^n, Z^n), there are around $2^{n(I(U_1; X_1|V_1) - I(U_1; V_2, Z|V_1) + I(U_2; X_2|V_2) - I(U_2; U_1, Z|V_2) + 2\epsilon)}$ jointly typical pairs of (U_1^n, U_2^n) in the constructed codebook. Then, we can follow similar steps in Lemma 4 to obtain that

$$\begin{aligned} &\frac{1}{n} H(U_1^n, U_2^n|V_1^n, V_2^n, Z^n, \mathcal{C}) \ge 3\epsilon + I(U_1; X_1|V_1) \\ &\quad - I(U_1; V_2, Z|V_1) + I(U_2; X_2|V_2) - I(U_2; U_1, Z|V_2) \\ &\quad = I(U_1, U_2; X_1, X_2|Z, V_1, V_2) + 3\epsilon. \end{aligned} \tag{133}$$

Thus, it follows that

$$\begin{aligned} &\frac{1}{n} H(X_1^n, X_2^n|M_{11}, M_{12}, M_{21}, M_{22}, Z^n, \mathcal{C}) \\ &\ge H(X_1, X_2|U_1, U_2, Z) + I(U_1, U_2; X_1, X_2|Z, V_1, V_2) \\ &\quad - I(U_1, U_2; X_1, X_2|Y, V_1, V_2) - 2\epsilon \\ &\ge H(X_1, X_2|U_1, U_2, Z) + I(U_1, U_2; Y|V_1, V_2) \\ &\quad - I(U_1, U_2; Z|V_1, V_2) - 2\epsilon. \end{aligned} \tag{134}$$

Similarly, we can obtain another scheme to achieve the other corner point, then we can use the time-sharing technique to show that the region defined by (33)-(37) is achievable.

D. Proof of Theorem 4

Given PMF $P_{X_1X_2Y} P_{U|X_1} P_{V|X_2}$ and a function g s.t. $D > E[d(f(X_1, X_2, Y), g(U, V, Y))] + \epsilon$, the achievability scheme is the same as that in the proof of Theorem 3, we only need to further analyze $\frac{1}{n} E[d(\mathbf{f}(X_1^n, X_2^n, Y^n), \mathbf{g}(\hat{U}^n, \hat{V}^n, Y^n))]$, which can be easily shown to be upper bounded by D with a high probability when n is large enough. We omit the details for brevity.

Outer Bound:

Following similar process of extending the proof of Theorem 1 to that of Theorem 2, the techniques used in Theorem 3 can be modified to prove Theorem 4 as follows. In this part, we set

$$U_{1i} := (M_1, X_1^{i-1}, Z^{i-1}, Y^{i-1}, Y_{i+1}^n), \tag{135}$$

$$V_{1i} := (M_1, Z^{i-1}, Y_{i+1}^n), \tag{136}$$

$$U_{2i} := (M_2, X_2^{i-1}, Z^{i-1}, , Y^{i-1}, Y_{i+1}^n), \quad (137)$$
$$V_{2i} := (M_2, Z^{i-1}, Y_{i+1}^n), \quad (138)$$

and define $U_1 := (U_{1J}, J)$ with J uniformly distributed in $[1:n]$ (V_1, U_2, V_2 are defined in a similar manner). We can conclude that

$$V_1 \to U_1 \to X_1 \to (X_2, Y, Z), \quad (139)$$

which follows from the following relationship:

$$\begin{aligned}&(X_1^n, Z^{i-1}, Y^{i-1}, Y_{i+1}^n) \to X_{1i} \to (X_{2i}, Y_i, Z_i)\\ \Rightarrow &(M_1, X_1^{i-1}, Z^{i-1}, Y^{i-1}, Y_{i+1}^n) \to X_{1i} \to (X_{2i}, Y_i, Z_i). \quad (140)\end{aligned}$$

Similarly, we also have $V_2 \to U_2 \to X_2 \to (X_1, Y, Z)$.

The proof of (39)-(42) can be obtained by following similar derivatives in the converse proof of Theorem 3. In particular, we will use the following Markov chains:

$$(X_{1i}, Y_i) \to (M_1, X_1^{i-1}, Y_{i+1}^n) \to (Y^{i-1}, Z^{i-1}), \quad (141)$$
$$(X_{2i}, Y_i) \to (M_2, X_2^{i-1}, Y_{i+1}^n) \to (Y^{i-1}, Z^{i-1}), \quad (142)$$
$$\begin{aligned}(X_{1i}, X_{2i}, Y_i) &\to (M_1, M_2, X_1^{i-1}, X_2^{i-1}, Y_{i+1}^n)\\ &\to (Y^{i-1}, Z^{i-1}), \quad (143)\end{aligned}$$

which follows from

$$(X_1^n, Y_i^n) \to X_1^{i-1} \to (Y^{i-1}, Z^{i-1}), \quad (144)$$
$$(X_2^n, Y_i^n) \to X_2^{i-1} \to (Y^{i-1}, Z^{i-1}), \quad (145)$$
$$(X_1^n, X_2^n, Y_i^n) \to (X_1^{i-1}, X_2^{i-1}) \to (Y^{i-1}, Z^{i-1}). \quad (146)$$

Specifically, the proof of (39) follows the similar derivatives of (107) by replacing Z^{i-1} with (Y^{i-1}, Z^{i-1}), and (40) follows in a similar manner, using the Markov chain relationships (141) and (142). Furthermore, with the Markov chain relationship (143), we can safely replace Z^{i-1} with (Y^{i-1}, Z^{i-1}) in (110) and (111), to obtain the derivation of (41) and (42) respectively. In addition, following similar steps from (84) to (88) by replacing X with (X_1, X_2), U with (U_1, U_2), V with (V_1, V_2) and M with (M_1, M_2), we can show the validity of (43), where we use the Markov chain (143) in the corresponding derivative as that in (85). Thus, in the sequel, we only show (44) as follows. Give D, we have

$$\begin{aligned}D &\geq \frac{1}{n} E\left[d(\mathbf{f}(X_1^n, X_2^n, Y^n), \hat{\mathbf{f}}(M_1, M_2, Y^n))\right] - \epsilon\\
&= \frac{1}{n} E\left[\sum_{i=1}^n d(f(X_{1i}, X_{2i}, Y_i), \hat{f}_i(M_1, M_2, Y^n))\right] - \epsilon\\
&\overset{(a)}{\geq} \frac{1}{n} E\left[\sum_{i=1}^n d(f(X_{1i}, X_{2i}, Y_i), g(M_1, M_2, Y^n, \right.\\
&\qquad \left. Z^{i-1}, {X_1}^{i-1}, {X_2}^{i-1}, i))\right] - \epsilon\\
&= \frac{1}{n} E\left[\sum_{i=1}^n d(f(X_{1i}, X_{2i}Y_i), g((U_1)_i, (U_2)_i, i, Y_i))\right] - \epsilon\\
&= E\left[\sum_{i=1}^n \frac{1}{n} d(f(X_{1i}, X_{2i}Y_i), g((U_1)_i, (U_2)_i, i, Y_i))\right] - \epsilon\\
&= E\left[d(f(X_1, X_2, Y), g(U_1, U_2, Y_I))\right] - \epsilon\\
&= E\left[d(f(X_1, X_2, Y), g(U_1, U_2, Y))\right] - \epsilon, \quad (147)\end{aligned}$$

where step (a) follows from the fact that $\hat{\mathbf{f}}$ is a function of (M_1, M_2, Y^n), thus there must exist some function, say g, such that the distortion decreases with more information is provided for each $i \in [1:n]$.

Hence, the converse proof is complete.

VI. Concluding Remarks

In this paper, we have considered the problem of function computation under privacy and secrecy constraints. We have first considered the special scenario where $\mathcal{X}_2 = \emptyset$, and have characterized the corresponding region for both the lossless and the lossy function computation cases. Then, we have generalized the obtained results into the more general scenarios and provided both outer bounds and inner bounds for the corresponding lossless and lossy cases.

Appendix A

Proof of Lemma 3: Denote the ϵ-jointly typical set of sequence pairs (U^n, V^n, Z^n) by $\mathcal{T}_\epsilon^n(U, V, Z)$, and the notation $\mathcal{T}_\epsilon^n(V, Z)$ in the sequel, follows in a similar manner. Set $\theta_1 = 0$ if $(U^n, V^n, Z^n) \in \mathcal{T}_\epsilon^n(U, V, Z)$, and $\theta_1 = 1$ otherwise. According to the scheme, we have, according to Markov lemma [39, Chapter 12], that $\Pr\{\theta_1 = 1\} \to 0$ as $n \to \infty$. Thus, we have $\Pr\{\theta_1 = 0\} \geq 1 - \epsilon$ when n is sufficiently large. It follows that

$$\begin{aligned}H(X^n|U^n, V^n, Z^n, \mathcal{C}) &\geq H(X^n|U^n, V^n, Z^n, \theta_1, \mathcal{C})\\
&= \Pr\{\theta_1 = 0\} H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C})\\
&\qquad + \Pr\{\theta_1 = 1\} H(X^n|U^n, V^n, Z^n, \theta_1 = 1, \mathcal{C})\\
&\geq (1 - \epsilon) H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C})\\
&= H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C})\\
&\qquad - \epsilon H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C})\\
&\geq H(X^n|U^n, V^n, Z^n, \theta_1 = 0, \mathcal{C}) - n\delta(\epsilon)\\
&= \sum_{z^n, \{v^n, u^n\} \in \mathcal{C}} \Pr\{u^n, v^n, z^n|\theta_1 = 0\} H(X^n|u^n, v^n, z^n) - n\delta(\epsilon)\\
&\geq \sum_{z^n, v^n, u^n \in \mathcal{C}} \Pr\{u^n, v^n, z^n|\theta_1 = 0\} n(H(X|U, V, Z) - \epsilon) - n\delta(\epsilon)\\
&\geq nH(X|U, V, Z) - n\epsilon - n\delta(\epsilon)\\
&= nH(X|U, Z) - n\epsilon - n\delta(\epsilon),\end{aligned}$$

for some value $\delta(\epsilon)$ of the same order of ϵ when n is sufficiently large. ∎

Proof of Lemma 4: Set $\theta_2 = 0$ if $(V^n, Z^n) \in \mathcal{T}_\epsilon^n(V, Z)$, and $\theta_2 = 1$ otherwise. Following the proof of Lemma 3, we have that

$$\begin{aligned}&H(U^n|V^n, Z^n, \mathcal{C})\\
&\qquad \geq \sum_{z^n, v^n \in \mathcal{C}} \Pr\{v^n, z^n|\theta_1 = 0\} H(U^n|v^n, z^n, \mathcal{C}) - n\epsilon. \quad (148)\end{aligned}$$

Now, set $\theta_3 = 0$ if $(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U, V, Z)$, and $\theta_3 = 1$ otherwise. Again, according to the Markov lemma, we have $\Pr\{\theta_3 = 0\} \geq 1 - \epsilon$ when n is sufficiently large. Then we have

$$\begin{aligned}H(U^n|v^n, z^n, \mathcal{C}) &\geq H(U^n|v^n, z^n, \theta_3, \mathcal{C})\\
&= \Pr\{\theta_3 = 0\} H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C})\\
&\qquad + \Pr\{\theta_3 = 1\} H(U^n|v^n, z^n, \theta_3 = 1, \mathcal{C})\\
&\geq H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C}) - n\delta(\epsilon). \quad (149)\end{aligned}$$

Denote $\mathrm{Num}(U^n|v^n, z^n)$ the number of sequences U^n that are generated by v^n and are jointly typical with (v^n, z^n). It is easy to verify that $\frac{1}{n}H(U^n|v^n, z^n, \theta_3 = 0, \mathcal{C}) \geq \log \mathrm{Num}(U^n|v^n, z^n) - \epsilon$, since each jointly typical U^n has the same, or close to be precise, probability to be the desired sequence. For each U^n generated by v^n, according the *Joint Typicality Lemma* [39, Chapter 2], we have

$$\Pr\{(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U, V, Z)\} \geq 2^{-n(I(U;Z|V)+\epsilon)}, \quad (150)$$

$$\Pr\{(U^n, v^n, z^n) \in \mathcal{T}_\epsilon^n(U, V, Z)\} \leq 2^{-n(I(U;Z|V)-\epsilon)} \quad (151)$$

if $(v^n, z^n) \in \mathcal{T}_\epsilon^n(V, Z)$. Thus, it follows that

$$\begin{aligned}\mathbb{E}[\mathrm{Num}((U^n|v^n, z^n))] &\geq 2^{n(I(U;X|V)+\epsilon)}2^{-n(I(U;Z|V)+\epsilon)} \\ &= 2^{n(I(U;X|V)-I(U;Z|V))}, \end{aligned} \quad (152)$$

and

$$\mathrm{Var}[\mathrm{Num}((U^n|v^n, z^n))] \leq 2^{n(I(U;X|V)-I(U;Z|V)+2\epsilon)}. \quad (153)$$

Thus, according to Chebyshev's inequality, we have

$$\begin{aligned}\Pr\{\mathrm{Num}((U^n|v^n, z^n)) &\leq \frac{1}{2}\mathbb{E}[\mathrm{Num}((U^n|v^n, z^n))]\} \\ &\leq 4 \cdot 2^{-n(I(U;X|V)-I(U;Z|V)-2\epsilon)} \leq \delta(\epsilon). \end{aligned} \quad (154)$$

Hence, we have

$$H(U^n|v^n, z^n, \mathcal{C}) \geq (1-\delta(\epsilon))n[I(U; X|V) - I(U; Z|V)], \quad (155)$$

which implies that

$$\frac{1}{n}H(U^n|V^n, Z^n, \mathcal{C}) \geq I(X; U|V) - I(Z; U|V) - 2\delta(\epsilon). \quad (156)$$

■

REFERENCES

[1] W. Tu and L. Lai, "Function computation with privacy constraints," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Oct. 2017, pp. 1672–1676.

[2] W. Tu and L. Lai, "On private lossy function computation," in *Proc. IEEE Workshop Signal Process. Adv. Wireless Commun.*, Kalamata, Greece, Jun. 2018, pp. 1–5.

[3] R. Appuswamy, M. Franceschetti, N. Karamchandani, and K. Zeger, "Network coding for computing: Cut-set bounds," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1015–1030, Feb. 2011.

[4] O. Ayaso, D. Shah, and M. A. Dahleh, "Information theoretic bounds for distributed computation over networks of point-to-point channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6020–6039, Dec. 2010.

[5] A. Giridhar and P. R. Kumar, "Computing and communicating functions over sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 23, pp. 755–764, Apr. 2005.

[6] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6337–6350, Oct. 2011.

[7] H. Tyagi and S. Watanabe, "A bound for multiparty secret key agreement and implications for a problem of secure Computing," in *Advances in Cryptology—EUROCRYPT*. Copenhagen, Denmark: Springer, May 2014, pp. 369–386.

[8] H. Tyagi and S. Watanabe, "Converses for secret key agreement and secure computing," *IEEE Trans. Inf. Theory*, vol. 61, no. 9, pp. 4809–4827, Sep. 2015.

[9] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3498–3516, Oct. 2007.

[10] H. Kowshik and P. R. Kumar, "Optimal function computation in directed and undirected graphs," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3407–3418, Jun. 2012.

[11] H. Kowshik and P. R. Kumar, "Optimal computation of symmetric Boolean functions in collocated networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 639–654, Apr. 2013.

[12] L. Ying, R. Srikant, and G. E. Dullerud, "Distributed symmetric function computation in noisy wireless sensor networks with binary data," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4826–4833, Dec. 2007.

[13] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

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

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

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

[17] M. Sefidgaran and A. Tchamkerten, "Computing a function of correlated sources: A rate region," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aug. 2011, pp. 1856–1860.

[18] M. Sefidgaran and A. Tchamkerten, "On cooperation in multi-terminal computation and rate distortion," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2012, pp. 766–770.

[19] M. Sefidgaran and A. Tchamkerten, "Distributed function computation over a rooted directed tree," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7135–7152, Dec. 2016.

[20] Z. Xiong, A. D. Liveris, and S. Cheng, "Distributed source coding for sensor networks," *IEEE Signal Process. Mag.*, vol. 21, no. 5, pp. 80–94, Sep. 2004.

[21] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 21, no. 3, pp. 294–300, May 1975.

[22] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[23] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, Nov. 1975.

[24] D. Gunduz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Inform. Theory Workshop*, Porto, Portugal, May 2008, pp. 169–173.

[25] Z. Xiong, A. D. Liveris, and Y. Yang, *Distributed Source Coding*. Hoboken, NJ, USA: Wiley, 2006.

[26] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[27] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Secur. Rev.*, vol. 26, no. 1, pp. 23–30, Jan. 2010.

[28] J. Li and G. AlRegib, "Rate-constrained distributed estimation in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 55, no. 5, pp. 1634–1643, May 2007.

[29] J. Ren, B. D. Boyle, G. Ku, S. Weber, and J. M. Walsh, "Overhead performance tradeoffs—A resource allocation perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3243–3269, Jun. 2016.

[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 2006.

[31] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, Jun. 2008.

[32] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[33] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, Dec. 2014.

[34] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 918–923, Nov. 1983.

[35] S. Satpathy and P. Cuff, "Secure coordination with a two-sided helper," in *Proc. IEEE Int. Symp. Inf. Theory*, Honolulu, HI, USA, Jul. 2014, pp. 406–410.

[36] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. Allerton Conf. Commun., Control, Computing*, Allerton, IL, USA, Sep. 2010, pp. 733–739.

[37] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, Jun. 2013.

[38] F. Naghibi, S. Salimi, and M. Skoglund, "The CEO problem with secrecy constraints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1234–1249, Jun. 2015.
[39] A. El Gamal and Y. Kim, *Network Information Theory*. New York, NY, USA: Cambridge Univ. Press, 2011.
[40] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[41] J. Vejnarovä, "Conditional independence and Markov properties in possibility theory," in *Proc. Conf. Uncertainty Artif. Intell.*, Stanford, CA, USA, Jun. 2000, pp. 609–616.

Wenwen Tu received the B.E. degree from University of Science and Technology of China, Hefei, China in 2013, and the Ph.D. degree from University of California, Davis in 2018.

Dr. Tu is currently with Black Sesame Technologies Inc., working as an AI Engineer. His research interests include information theory, stochastic learning, machine learning.

Lifeng Lai (M'07) received the B.E. and M.E. degrees from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the Ph.D. from The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at Princeton University from 2007 to 2009, an assistant professor at University of Arkansas, Little Rock from 2009 to 2012, and an assistant professor at Worcester Polytechnic Institute from 2012 to 2016. Since 2016, he has been an associate professor at University of California, Davis. Dr. Lai's research interests include information theory, stochastic signal processing and their applications in wireless communications, security and other related areas.

Dr. Lai was a Distinguished University Fellow of the Ohio State University from 2004 to 2007. He is a co-recipient of the Best Paper Award from IEEE Global Communications Conference (Globecom) in 2008, the Best Paper Award from IEEE Conference on Communications (ICC) in 2011 and the Best Paper Award from IEEE Smart Grid Communications (SmartGridComm) in 2012. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012. He served as a Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security from 2012 to 2013, and served as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2013 to 2018. He is currently serving as an Associate Editor for IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY.