Multiple Noisy Private Remote Source Observations for Secure Function Computation

Onur Günlü[1], Matthieu Bloch[2], and Rafael F. Schaefer[1]

[1]Chair of Communications Engineering and Security, University of Siegen,
{onur.guenlue, rafael.schaefer}@uni-siegen.de
[2]School of Electrical and Computer Engineering, Georgia Institute of Technology,
matthieu.bloch@ece.gatech.edu

***Abstract*—The problem of reliable function computation is extended by imposing privacy, secrecy, and storage constraints on a remote source whose noisy measurements are observed by multiple parties. The main additions to the classic function computation problem include 1) privacy leakage to an eavesdropper is measured with respect to the remote source rather than the transmitting terminals' observed sequences; 2) the information leakage to a fusion center with respect to the remote source is considered as another privacy leakage metric; 3) two transmitting node observations are used to compute a function. Inner and outer bounds on the rate regions are derived for lossless single-function computation with two transmitting nodes, which recover previous results in the literature, and for special cases that consider invertible functions exact rate regions are characterized.**

I. Introduction

We consider function computation scenarios in a network with multiple nodes involved. Each node observes a random sequence and all observed random sequences are modeled to be correlated. Recent advancements in network function virtualization [1] and distributed machine learning applications [2] make function computation in a wireless network via software defined networking an important practical problem that should be tackled to improve the performance of future communication systems. In a classic function computation scenario, the nodes exchange messages through authenticated, noiseless, and public communication links, which results in undesired information leakage about the function computed [3]–[5]. Furthermore, it is possible to reduce the amount of public communications [6], [7], e.g., by using distributed lossless source coding (or Slepian-Wolf coding) techniques [8]; see [9]–[13] for several extensions. A decrease in public communications is important also to limit the information about the computed function leaked to an eavesdropper in the same network, i.e., *secrecy leakage*. In addition to the public messages, an eavesdropper has generally access to a random sequence correlated with other sequences; see [14]–[16] for various secure function computation extensions.

An important addition to the secure function computation model is a *privacy* constraint that measures the amount of information about the observed sequence leaked to an eavesdropper [17]. Providing privacy is necessary to ensure confidentiality of a private sequence that can be re-used for future function computations [18], [19]. An extension of the results in [17] are given in [20], where two privacy constraints are considered on a remote source whose different noisy measurements are observed by multiple nodes in the same network. The extension in [20] is different from the previous secure and private function computation models due to the posit that there exists a remote source that is the main reason for the correlation between the random sequences observed by the nodes in the network. It is illustrated via practical examples that considering a remote source hinders unexpected decrease in reliability and unnoticed secrecy leakage [19]. Similarly, such a hidden source model is proposed, e.g., in [21] for biometric secrecy and in [22], [23] for user or device authentication problems. It is shown in [20] that with such a hidden source model two different privacy leakage rate values should be limited, unlike a single constraint considered in [17].

We consider a private remote source whose noisy versions are used for secure function computation. The main additions to the problem are to compute one function we consider that two nodes transmit public indices to a fusion center. In [20], for each function computation one node sends a public index to a fusion center. In [17], cases with two transmitting nodes for function computation are considered for a visible source model, whose results are improved in this work for a remote source model with an additional privacy leakage constraint. We provide inner and outer bounds for the single function computation model with two transmitting nodes under one secrecy, two privacy, two storage, and one reliability constraint. We use the output statistics of random binning (OSRB) method [24] to simplify the proofs, as in [20], and characterize the rate region for invertible functions.

II. System Model

We consider the function computation model with two transmitting nodes illustrated in Fig. 1. Noisy measurements $\widetilde{X}_1^n$ and $\widetilde{X}_2^n$ of an independent and identically distributed (i.i.d.) remote source $X^n \sim P_X^n$ through memoryless channels $P_{\widetilde{X}_1|X}$ and $P_{\widetilde{X}_2|X}$, respectively, are observed by two legitimate nodes in a network. Similarly, other noisy measurements Y^n and Z^n of the same remote source are observed by, respectively, the fusion center and eavesdropper (Eve) through another memoryless channel $P_{YZ|X}$. Encoders $\mathsf{Enc}_1(\cdot)$ and $\mathsf{Enc}_2(\cdot)$ of the legitimate nodes send indices W_1 and W_2, respectively, to

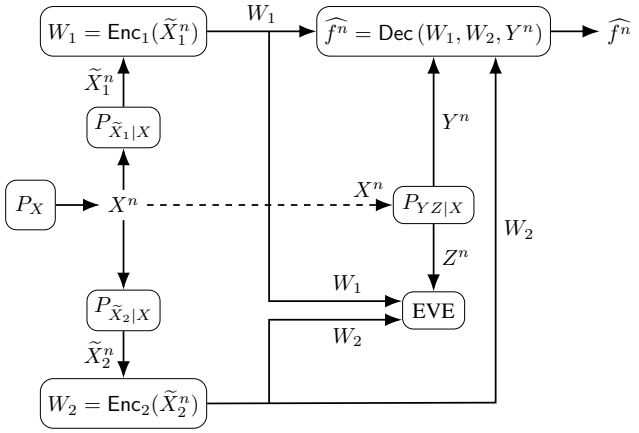

Fig. 1. Single-function computation with two transmitting nodes.

the fusion center over public communication links with storage rate constraints. The fusion center decoder $\mathsf{Dec}(\cdot)$ then uses its observed noisy sequence Y^n and the public indices W_1 and W_2 to reliably estimate a function $f^n(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n)$ such that

$$f^n(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n) = \{f(\widetilde{X}_{1,i}, \widetilde{X}_{2,i}, Y_i)\}_{i=1}^n. \tag{1}$$

The source and measurement alphabets are finite sets.

A natural secrecy leakage constraint is to minimize the information leakage about the function output $f^n(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n)$ to Eve. However, its analysis depends on the specific function $f(\cdot,\cdot,\cdot)$ computed, so we impose another secrecy leakage constraint that does not depend on the function used and that provides an upper bound for secrecy leakage for all functions, as considered in [17], [20]. We impose two privacy leakage constraints to minimize the information leakage about X^n to the fusion center and Eve as well as public storage constraints that minimize the rate of storage for transmitting nodes.

Definition 1. A tuple $(R_{\rm s}, R_{\rm w,1}, R_{\rm w,2}, R_{\ell,\rm Dec}, R_{\ell,\rm Eve})$ is *achievable* if, for any $\delta > 0$, there exist $n \geq 1$, two encoders, and one decoder such that

$$\Pr\left[f^n(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n) \neq \widehat{f^n}\right] \leq \delta \qquad \text{(reliability)} \tag{2}$$

$$I(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n; W_1, W_2|Z^n) \leq n(R_{\rm s} + \delta) \qquad \text{(secrecy)} \tag{3}$$

$$\log\left|\mathcal{W}_1\right| \leq n(R_{\rm w,1} + \delta) \qquad \text{(storage 1)} \tag{4}$$

$$\log\left|\mathcal{W}_2\right| \leq n(R_{\rm w,2} + \delta) \qquad \text{(storage 2)} \tag{5}$$

$$I(X^n; W_1, W_2|Y^n) \leq n(R_{\ell,\rm Dec} + \delta) \qquad \text{(privacyDec)} \tag{6}$$

$$I(X^n; W_1, W_2|Z^n) \leq n(R_{\ell,\rm Eve} + \delta) \qquad \text{(privacyEve)}. \tag{7}$$

The region $\mathcal{R}$ is the closure of the set of all achievable tuples.

III. Inner and Outer Bounds

We first extend the notion of *admissibility* for a random variable defined in [6] for a single auxiliary random variable to two auxiliary random variables, used in the inner and outer bounds below; see also [17, Theorem 3].

Definition 2. A pair of (vector) random variables (U_1, U_2) is admissible for a function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ if $H(f(\widetilde{X}_1, \widetilde{X}_2, Y)|\, U_1, U_2, Y) = 0$ and both $U_1 - \widetilde{X}_1 - (\widetilde{X}_2, Y)$ and $U_2 - \widetilde{X}_2 - (\widetilde{X}_1, Y)$ form Markov chains.

Given any $a \in \mathbb{R}$, define $[a]^- = \min\{a, 0\}$. We next provide inner and outer bounds for the region $\mathcal{R}$; see Section IV for a proof sketch.

Theorem 1. (Inner Bound): *An achievable region is the union over all P_Q, $P_{V_1|Q}$, $P_{V_2|Q}$, $P_{U_1|V_1}$, $P_{U_2|V_2}$, $P_{\widetilde{X}_1|U_1}$, and $P_{\widetilde{X}_2|U_2}$ of the rate tuples $(R_s, R_{w,1}, R_{w,2}, R_{\ell,Dec}, R_{\ell,Eve})$ such that (U_1, U_2) pair is admissible for the function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ and*

$$R_s \geq \Big[I(U_1,U_2;Z|V_1,V_2,Q) - I(U_1,U_2;Y|V_1,V_2,Q)\Big]^- + I(U_1,U_2;\widetilde{X}_1,\widetilde{X}_2|Z) \tag{8}$$

$$R_{w,1} \geq I(V_1;\widetilde{X}_1|V_2,Y) + I(U_1;\widetilde{X}_1|V_1,U_2,Y) \tag{9}$$

$$R_{w,2} \geq I(V_2;\widetilde{X}_2|V_1,Y) + I(U_2;\widetilde{X}_2|U_1,V_2,Y) \tag{10}$$

$$R_{w,1} + R_{w,2} \geq I(U_2;\widetilde{X}_2|U_1,V_2,Y) + I(U_1;\widetilde{X}_1|V_1,V_2,Y) + I(V_2;\widetilde{X}_2|V_1,Y) + I(V_1;\widetilde{X}_1|Y) \tag{11}$$

$$R_{\ell,Dec} \geq I(U_1,U_2;X|Y) \tag{12}$$

$$R_{\ell,Eve} \geq \Big[I(U_1,U_2;Z|V_1,V_2,Q) - I(U_1,U_2;Y|V_1,V_2,Q)\Big]^- + I(U_1,U_2;X|Z) \tag{13}$$

where $P_{QV_1V_2U_1U_2\widetilde{X}_1\widetilde{X}_2XYZ}$ is equal to

$$P_{Q|V_1V_2}P_{V_1|U_1}P_{U_1|\widetilde{X}_1}P_{\widetilde{X}_1|X}P_{V_2|U_2}P_{U_2|\widetilde{X}_2}P_{\widetilde{X}_2|X}P_XP_{YZ|X}. \tag{14}$$

(Outer Bound): *An outer bound for the region $\mathcal{R}$ is the union of the rate tuples in (8), (11)-(13), and*

$$R_{w,1} \geq I(V_1;\widetilde{X}_1|V_2,Y) + I(U_1;\widetilde{X}_1|V_1,U_2,Y) - I(V_1;V_2|\widetilde{X}_1,Y) - I(U_1;U_2|\widetilde{X}_1,Y,V_1) \tag{15}$$

$$R_{w,2} \geq I(V_2;\widetilde{X}_2|V_1,Y) + I(U_2;\widetilde{X}_2|U_1,V_2,Y) - I(V_2;V_1|\widetilde{X}_2,Y) - I(U_2;U_1|\widetilde{X}_2,Y,V_2) \tag{16}$$

over all P_Q, $P_{V_1|Q}$, $P_{V_2|Q}$, $P_{U_1|V_1}$, $P_{U_2|V_2}$, $P_{\widetilde{X}_1|U_1}$, and $P_{\widetilde{X}_2|U_2}$ such that (U_1, U_2) pair is admissible for the function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ and

$$(Q, V_1) - U_1 - \widetilde{X}_1 - X - (\widetilde{X}_2, Y, Z) \tag{17}$$

$$(Q, V_2) - U_2 - \widetilde{X}_2 - X - (\widetilde{X}_1, Y, Z) \tag{18}$$

form Markov chains. One can limit the cardinalities to $|\mathcal{Q}| \leq 2$, $|\mathcal{V}_1| \leq |\widetilde{X}_1|+6$, $|\mathcal{V}_2| \leq |\widetilde{X}_2|+6$, $|\mathcal{U}_1| \leq (|\widetilde{X}_1|+6)^2$, $|\mathcal{U}_2| \leq (|\widetilde{X}_2|+6)^2$.

We remark that if the joint probability distribution in (14) is imposed on the outer bound, (15) and (16) recover (9) and (10), respectively, because then $(V_1, U_1) - \widetilde{X}_1 - (Y, U_2, V_2)$ and $(V_2, U_2) - \widetilde{X}_2 - (Y, U_1, V_1)$ form Markov chains for (14). However, the outer bound that satisfies (17) and (18) defines a rate region that is in general larger than the rate region defined by the inner bound that satisfies (14). Thus, inner and outer bounds generally differ. The results in Theorem 1 recovers

previous results including [17, Theorem 3] and, naturally, also other results that are recovered by these previous results such as the Slepian-Wolf coding problem.

Suppose now we impose the condition that the function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ is invertible, i.e., $H(\widetilde{X}_1, \widetilde{X}_2 | f(\widetilde{X}_1, \widetilde{X}_2, Y), Y) = 0$ as discussed in [10], [25]. We provide in Corollary 1 below the exact rate region for the single-function computation problem with two transmitting nodes when the function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ is invertible. The proof of Corollary 1 follows from Theorem 1 by assigning $U_1 = \widetilde{X}_1$, $U_2 = \widetilde{X}_2$, and constant V_1 and V_2.

Corollary 1. *The region $\mathcal{R}$ when $f(\widetilde{X}_1, \widetilde{X}_2, Y)$ is an invertible function is the set of all tuples $(R_s, R_{w,1}, R_{w,2}, R_{\ell,Dec}, R_{\ell,Eve})$ satisfying*

$$R_s \geq \big[I(\widetilde{X}_1, \widetilde{X}_2; Z|Q) - I(\widetilde{X}_1, \widetilde{X}_2; Y|Q)\big]^- + H(\widetilde{X}_1, \widetilde{X}_2|Z) \tag{19}$$

$$R_{w,1} \geq H(\widetilde{X}_1|\widetilde{X}_2, Y) \tag{20}$$

$$R_{w,2} \geq H(\widetilde{X}_2|\widetilde{X}_1, Y) \tag{21}$$

$$R_{w,1} + R_{w,2} \geq H(\widetilde{X}_1, \widetilde{X}_2|Y) \tag{22}$$

$$R_{\ell,Dec} \geq I(\widetilde{X}_1, \widetilde{X}_2; X|Y) \tag{23}$$

$$R_{\ell,Eve} \geq \big[I(\widetilde{X}_1, \widetilde{X}_2; Z|Q) - I(\widetilde{X}_1, \widetilde{X}_2; Y|Q)\big]^- + I(\widetilde{X}_1, \widetilde{X}_2; X|Z) \tag{24}$$

where $Q - (\widetilde{X}_1, \widetilde{X}_2) - X - (Y, Z)$ form a Markov chain. One can limit the cardinality to $|\mathcal{Q}| \leq 2$.

IV. Proof of Theorem 1

A. Inner Bound Proof Sketch

Proof. The OSRB method [24] is used by applying the steps given in [26, Section 1.6]. Let $(V_1^n, V_2^n, U_1^n, U_2^n, \widetilde{X}_1^n, \widetilde{X}_2^n, X^n, Y^n, Z^n)$ be i.i.d. according to $P_{V_1V_2U_1U_2\widetilde{X}_1\widetilde{X}_2XYZ}$ that can be obtained from (14) with fixed $P_{U_1|\widetilde{X}_1}$, $P_{V_1|U_1}$, $P_{U_2|\widetilde{X}_2}$, and $P_{V_2|U_2}$ such that the pair (U_1, U_2) is admissible for a function $f(\widetilde{X}_1, \widetilde{X}_2, Y)$, so (U_1^n, U_2^n) is also admissible due to i.i.d. random variables.

To each v_1^n assign two random bin indices $(F_{\mathrm{v}_1}, W_{\mathrm{v}_1})$ such that $F_{\mathrm{v}_1} \in [1 : 2^{n\widetilde{R}_{\mathrm{v}_1}}]$ and $W_{\mathrm{v}_1} \in [1 : 2^{nR_{\mathrm{v}_1}}]$. Furthermore, to each u_1^n assign two random indices $(F_{\mathrm{u}_1}, W_{\mathrm{u}_1})$ such that $F_{\mathrm{u}_1} \in [1 : 2^{n\widetilde{R}_{\mathrm{u}_1}}]$ and $W_{\mathrm{u}_1} \in [1 : 2^{nR_{\mathrm{u}_1}}]$. Similarly, random indices $(F_{\mathrm{v}_2}, W_{\mathrm{v}_2})$ and $(F_{\mathrm{u}_2}, W_{\mathrm{u}_2})$ are assigned to each v_2^n and u_2^n, respectively. The indices $F_1 = (F_{\mathrm{v}_1}, F_{\mathrm{u}_1})$, and $F_2 = (F_{\mathrm{v}_2}, F_{\mathrm{u}_2})$ represent the public choice of two encoders and one decoder, whereas $W_1 = (W_{\mathrm{v}_1}, W_{\mathrm{u}_1})$ and $W_2 = (W_{\mathrm{v}_2}, W_{\mathrm{u}_2})$ are the public messages sent by the encoders $\mathsf{Enc}_1(\cdot)$ and $\mathsf{Enc}_2(\cdot)$, respectively, to the fusion center.

We consider the following decoding order: 1) observing $(Y^n, F_{\mathrm{v}_1}, W_{\mathrm{v}_1})$, the decoder $\mathsf{Dec}(\cdot)$ estimates V_1^n as $\widehat{V}_1^n$; 2) observing $(Y^n, \widehat{V}_1^n, F_{\mathrm{v}_2}, W_{\mathrm{v}_2})$, the decoder estimates V_2^n as $\widehat{V}_2^n$; 3) observing $(Y^n, \widehat{V}_1^n, \widehat{V}_2^n, F_{\mathrm{u}_1}, W_{\mathrm{u}_1})$, the decoder estimates U_1^n as $\widehat{U}_1^n$; 4) observing $(Y^n, \widehat{V}_1^n, \widehat{V}_2^n, \widehat{U}_1^n, F_{\mathrm{u}_2}, W_{\mathrm{u}_2})$, the decoder estimates U_2^n as $\widehat{U}_2^n$. By swapping indices 1 and 2 in the decoding order another corner point in the achievable rate region is obtained, so we analyze the given decoding order but also provide the results for the other corner point.

Consider Step 1 in the decoding order given above. Using a Slepian-Wolf (SW) [8] decoder, one can reliably estimate V_1^n from $(Y^n, F_{\mathrm{v}_1}, W_{\mathrm{v}_1})$ such that the expected value of the error probability taken over the random bin assignments vanishes when $n \to \infty$, if we have [24, Lemma 1]

$$\widetilde{R}_{\mathrm{v}_1} + R_{\mathrm{v}_1} > H(V_1|Y). \tag{25}$$

Similarly, Step 2, 3, and 4 estimations are reliable if we have

$$\widetilde{R}_{\mathrm{v}_2} + R_{\mathrm{v}_2} > H(V_2|V_1, Y) \tag{26}$$

$$\widetilde{R}_{\mathrm{u}_1} + R_{\mathrm{u}_1} > H(U_1|V_1, V_2, Y) \tag{27}$$

$$\widetilde{R}_{\mathrm{u}_2} + R_{\mathrm{u}_2} > H(U_2|V_1, V_2, U_1, Y) \overset{(a)}{=} H(U_2|V_2, U_1, Y) \tag{28}$$

where (a) follows from the Markov chain $V_1 - U_1 - (U_2, V_2, Y)$. Therefore, (2) is satisfied if (25)-(28) are satisfied.

The public index F_{v_1} is almost independent of $\widetilde{X}_1^n$, so it is almost independent of $(\widetilde{X}_1^n, \widetilde{X}_2^n, X^n, Y^n, Z^n)$, if we have [24, Theorem 1]

$$\widetilde{R}_{\mathrm{v}_1} < H(V_1|\widetilde{X}_1) \tag{29}$$

because then the expected value, which is taken over the random bin assignments, of the variational distance between the joint probability distributions $\mathrm{Unif}[1 : 2^{n\widetilde{R}_{\mathrm{v}_1}}] \cdot P_{\widetilde{X}_1^n}$ and $P_{F_{\mathrm{v}_1}\widetilde{X}_1^n}$ to vanish when $n \to \infty$. Furthermore, the public index F_{u_1} is almost independent of $(V_1^n, \widetilde{X}_1^n)$, so it is almost independent of $(V_1^n, \widetilde{X}_1^n, \widetilde{X}_2^n, X^n, Y^n, Z^n)$, if we have

$$\widetilde{R}_{\mathrm{u}_1} < H(U_1|V_1, \widetilde{X}_1). \tag{30}$$

Similarly, F_{v_2} is almost independent of $\widetilde{X}_2^n$ if we have

$$\widetilde{R}_{\mathrm{v}_2} < H(V_2|\widetilde{X}_2) \tag{31}$$

and F_{u_2} is almost independent of $(V_2^n, \widetilde{X}_2^n)$ if we have

$$\widetilde{R}_{\mathrm{u}_2} < H(U_2|V_2, \widetilde{X}_2). \tag{32}$$

To satisfy (25)-(32), for any $\epsilon > 0$ we fix

$$\widetilde{R}_{\mathrm{v}_1} = H(V_1|\widetilde{X}_1) - \epsilon \tag{33}$$

$$R_{\mathrm{v}_1} = I(V_1; \widetilde{X}_1) - I(V_1; Y) + 2\epsilon \tag{34}$$

$$\widetilde{R}_{\mathrm{v}_2} = H(V_2|\widetilde{X}_2) - \epsilon \tag{35}$$

$$R_{\mathrm{v}_2} = I(V_2; \widetilde{X}_2) - I(V_2; V_1, Y) + 2\epsilon \tag{36}$$

$$\widetilde{R}_{\mathrm{u}_1} = H(U_1|V_1, \widetilde{X}_1) - \epsilon \tag{37}$$

$$R_{\mathrm{u}_1} = I(U_1; \widetilde{X}_1|V_1) - I(U_1; V_2, Y|V_1) + 2\epsilon \tag{38}$$

$$\widetilde{R}_{\mathrm{u}_2} = H(U_2|V_2, \widetilde{X}_2) - \epsilon \tag{39}$$

$$R_{\mathrm{u}_2} = I(U_2; \widetilde{X}_2|V_2) - I(U_2; U_1, Y|V_2) + 2\epsilon. \tag{40}$$

Public Message (Storage) Rates: (34) and (38) result in a public message (storage) rate R_{w_1} of

$$\begin{aligned} R_{\mathrm{w}_1} &= R_{\mathrm{v}_1} + R_{\mathrm{u}_1} \\ &\overset{(a)}{=} I(V_1; \widetilde{X}_1|Y) + H(U_1|V_1, V_2, Y) - H(U_1|V_1, \widetilde{X}_1) + 4\epsilon \\ &\overset{(b)}{=} I(V_1; \widetilde{X}_1|Y) + I(U_1; \widetilde{X}_1|V_1, V_2, Y) + 4\epsilon \end{aligned} \tag{41}$$

where (a) follows because $V_1 - \widetilde{X}_1 - Y$ form a Markov chain and (b) follows because $U_1 - (V_1, \widetilde{X}_1) - (V_2, Y)$ form a Markov chain. Furthermore, (36) and (40) result in a storage rate R_{w_2} of

$$\begin{aligned}
R_{\mathrm{w}_2} &= R_{\mathrm{v}_2} + R_{\mathrm{u}_2} \\
&\overset{(a)}{=} I(V_2; \widetilde{X}_2|V_1, Y) + H(U_2|U_1, V_2, Y) - H(U_2|V_2, \widetilde{X}_2) + 4\epsilon \\
&\overset{(b)}{=} I(V_2; \widetilde{X}_2|V_1, Y) + I(U_2; \widetilde{X}_2|U_1, V_2, Y) + 4\epsilon \qquad (42)
\end{aligned}$$

where (a) follows from the Markov chain $V_2 - \widetilde{X}_2 - (V_1, Y)$ and (b) from $U_2 - (V_2, \widetilde{X}_2) - (U_1, Y)$. We remark that if the indices 1 and 2 in the decoding order given above are swapped, the other corner point with

$$R'_{\mathrm{w}_1} = I(V_1; \widetilde{X}_1|V_2, Y) + I(U_1; \widetilde{X}_1|U_2, V_1, Y) + 4\epsilon \qquad (43)$$

$$R'_{\mathrm{w}_2} = I(V_2; \widetilde{X}_2|Y) + I(U_2; \widetilde{X}_2|V_1, V_2, Y) + 4\epsilon \qquad (44)$$

is achieved.

Privacy Leakage to Decoder: We have

$$\begin{aligned}
&I(X^n; W_1, W_2, F_1, F_2|Y^n) \\
&= I(X^n; W_1, W_2|F_1, F_2, Y^n) + I(X^n; F_1, F_2|Y^n) \\
&\overset{(a)}{\leq} H(X^n|Y^n) \\
&\quad - H(X^n|W_1, W_2, F_1, F_2, V_1^n, V_2^n, U_1^n, U_2^n, Y^n) + 4\epsilon_n \\
&\overset{(b)}{=} H(X^n|Y^n) - H(X^n|U_1^n, U_2^n, Y^n) + 4\epsilon_n \\
&\overset{(c)}{=} nI(U_1, U_2; X|Y) + 4\epsilon_n \qquad (45)
\end{aligned}$$

where (a) follows for some $\epsilon_n > 0$ with $\epsilon_n \to 0$ when $n \to \infty$ because

$$\begin{aligned}
&I(X^n; F_1, F_2|Y^n) \\
&= I(X^n; F_{\mathrm{v}_1}|Y^n) + I(X^n; F_{\mathrm{u}_1}|F_{\mathrm{v}_1}, Y^n) \\
&\quad + I(X^n; F_{\mathrm{v}_2}|F_{\mathrm{v}_1}, F_{\mathrm{u}_1}, Y^n) \\
&\quad + I(X^n; F_{\mathrm{u}_2}|F_{\mathrm{v}_1}, F_{\mathrm{u}_1}, F_{\mathrm{v}_2}, Y^n) \leq 4\epsilon_n \qquad (46)
\end{aligned}$$

since 1) by (29) F_{v_1} is almost independent of (X^n, Y^n); 2) by (30) F_{u_1} is almost independent of (V_1^n, X^n, Y^n) and because V_1^n determines F_{v_1}; 3) by (31) F_{v_2} is almost independent of (U_1^n, V_1^n, X^n, Y^n) and because (V_1^n, U_1^n) determine $(F_{\mathrm{v}_1}, F_{\mathrm{u}_1})$; 4) by (32) F_{u_2} is almost independent of $(V_2^n, U_1^n, V_1^n, X^n, Y^n)$ and because (V_1^n, U_1^n, V_2^n) determine $(F_{\mathrm{v}_1}, F_{\mathrm{u}_1}, F_{\mathrm{v}_2})$, (b) follows because $(V_1^n, V_2^n, U_1^n, U_2^n)$ determine (W_1, W_2, F_1, F_2) and from the Markov chains $V_1^n - U_1^n - (X^n, Y^n, U_2^n, V_2^n)$ and $V_2^n - U_2^n - (X^n, Y^n, U_1^n)$, and (c) follows because (X^n, U_1^n, U_2^n, Y^n) are i.i.d.

Privacy Leakage to Eve: We have

$$\begin{aligned}
&I(X^n; W_1, W_2, F_1, F_2|Z^n) \\
&\overset{(a)}{=} H(W_1, W_2, F_1, F_2|Z^n) - H(W_1, W_2, F_1, F_2|X^n) \\
&\overset{(b)}{=} H(W_1, W_2, F_1, F_2|Z^n) \\
&\quad - H(W_{u_1}, F_{u_1}, W_{u_2}, F_{u_2}, V_1^n, V_2^n|X^n) \\
&\quad + H(V_1^n|W_1, W_2, F_1, F_2, X^n) \\
&\quad + H(V_2^n|V_1^n, W_1, W_2, F_1, F_2, X^n) \\
&\overset{(c)}{\leq} H(W_1, W_2, F_1, F_2|Z^n) \\
&\quad - H(W_{u_1}, F_{u_1}, W_{u_2}, F_{u_2}, V_1^n, V_2^n|X^n) + 2n\epsilon'_n \\
&\overset{(d)}{=} H(W_1, W_2, F_1, F_2|Z^n) - H(U_1^n, U_2^n, V_1^n, V_2^n|X^n) \\
&\quad + H(U_1^n|W_{u_1}, F_{u_1}, W_{u_2}, F_{u_2}, V_1^n, V_2^n, X^n) \\
&\quad + H(U_2^n|U_1^n, W_{u_1}, F_{u_1}, W_{u_2}, F_{u_2}, V_1^n, V_2^n, X^n) + 2n\epsilon'_n \\
&\overset{(e)}{\leq} H(W_1, W_2, F_1, F_2|Z^n) - H(U_1^n, U_2^n, V_1^n, V_2^n|X^n) + 4n\epsilon'_n \\
&\overset{(f)}{=} H(W_1, W_2, F_1, F_2|Z^n) \\
&\quad - nH(U_1, U_2, V_1, V_2|X) + 4n\epsilon'_n \qquad (47)
\end{aligned}$$

where (a) follows because $(W_1, W_2, F_1, F_2) - X^n - Z^n$ form a Markov chain, (b) follows since (V_1^n, V_2^n) determine $(F_{v_1}, W_{v_1}, F_{v_2}, W_{v_2})$, (c) follows for some $\epsilon'_n > 0$ such that $\epsilon'_n \to 0$ when $n \to \infty$ because (F_{v_1}, W_{v_1}, X^n) can reliably recover V_1^n by (25), and similarly because $(F_{v_2}, W_{v_2}, V_1^n, X^n)$ can reliably recover V_2^n by (26) both due to the Markov chain $(V_1^n, V_2^n) - X^n - Y^n$, (d) follows because (U_1^n, U_2^n) determine $(F_{u_1}, W_{u_1}, F_{u,2}, W_{u_2})$, (e) follows because $(F_{u_1}, W_{u_1}, V_1^n, V_2^n, X^n)$ can reliably recover U_1^n by (27) and the inequality $H(U_1|V_1, V_2, Y) \geq H(U_1|V_1, V_2, X)$ that follows from

$$\begin{aligned}
&I(U_1; V_1, V_2, X) - I(U_1; V_1, V_2, Y) \\
&\geq I(U_1; V_1, V_2, X) - I(U_1; V_1, V_2, Y, X) = 0 \qquad (48)
\end{aligned}$$

since $U_1 - (V_1, V_2, X) - Y$ form a Markov chain. Similarly, $(F_{u_2}, W_{u_2}, V_1^n, V_2^n, U_1^n, X^n)$ can reliably recover U_2^n by (28) and the inequality $H(U_2|V_1, V_2, U_1, Y) \geq H(U_2|V_1, V_2, U_1, X)$ that can be proved entirely similarly to (48) by using the Markov chain $U_2 - (V_1, V_2, U_1, X) - Y$, and (f) follows because $(U_1^n, U_2^n, V_1^n, V_2^n, X^n)$ are i.i.d.

In (47), obtaining single letter bounds on the term $H(W_1, W_2, F_1, F_2|Z^n)$ requires analysis of numerous decodability cases, whereas there are only six different decodability cases analyzed in [20] for secure function computation with a single transmitting node. To simplify our analysis by applying the results in [20], we combine the decoding order Steps 1 and 2 given above such that (V_1, V_2) are treated jointly and, similarly, we combine Steps 3 and 4 such that (U_1, U_2) are treated jointly. Using the combined steps, we can consider the six decodability cases analyzed in [20, Section V-A] by replacing V^n with (V_1^n, V_2^n) and U^n with (U_1^n, U_2^n), respectively, in the proof. Since in (47) the second term $-nH(U_1, U_2, V_1, V_2|X)$ can be obtained by applying the same replacement to the second term in [20, Eq. (54)], we obtain from (47) and these decodability analyses that

$$\begin{aligned}
&I(X^n; W_1, W_2, F_1, F_2|Z^n) \\
&\leq n([I(U_1, U_2; Z|V_1, V_2) - I(U_1, U_2; Y|V_1, V_2) + \epsilon]^- \\
&\quad + I(U_1, U_2; X|Z) + 4\epsilon'_n + \epsilon''_n) \qquad (49)
\end{aligned}$$

for some $\epsilon''_n > 0$ such that $\epsilon''_n \to 0$ when $n \to \infty$.

Secrecy Leakage (to Eve): We obtain

$$
\begin{aligned}
&I(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n; W_1, W_2, F_1, F_2 | Z^n) \\
&\overset{(a)}{=} H(W_1, W_2, F_1, F_2 | Z^n) - H(W_1, W_2, F_1, F_2 | \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\overset{(b)}{=} H(W_1, W_2, F_1, F_2 | Z^n) \\
&\quad - H(W_{u_1}, W_{u_2}, F_{u_1}, F_{u_2}, V_1^n, V_2^n | \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\quad + H(V_1^n | W_1, W_2, F_1, F_2, \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\quad + H(V_2^n | V_1^n, W_1, W_2, F_1, F_2, \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\overset{(c)}{\leq} H(W_1, W_2, F_1, F_2 | Z^n) \\
&\quad - H(W_{u_1}, W_{u_2}, F_{u_1}, F_{u_2}, V_1^n, V_2^n | \widetilde{X}_1^n, \widetilde{X}_2^n) + 2n\epsilon_n' \\
&\overset{(d)}{=} H(W_1, W_2, F_1, F_2 | Z^n) \\
&\quad - H(U_1^n, U_2^n, V_1^n, V_2^n | \widetilde{X}_1^n, \widetilde{X}_2^n) + 2n\epsilon_n' \\
&\quad + H(U_1^n | W_{u_1}, W_{u_2}, F_{u_1}, F_{u_2}, V_1^n, V_2^n, \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\quad + H(U_2^n | U_1^n, W_{u_1}, W_{u_2}, F_{u_1}, F_{u_2}, V_1^n, V_2^n, \widetilde{X}_1^n, \widetilde{X}_2^n) \\
&\overset{(e)}{\leq} H(W_1, W_2, F_1, F_2 | Z^n) \\
&\quad - H(U_1^n, U_2^n, V_1^n, V_2^n | \widetilde{X}_1^n, \widetilde{X}_2^n) + 4n\epsilon_n' \\
&\overset{(f)}{\leq} H(W_1, W_2, F_1, F_2 | Z^n) \\
&\quad - nH(U_1, U_2, V_1, V_2 | \widetilde{X}_1, \widetilde{X}_2) + 4n\epsilon_n' \qquad (50)
\end{aligned}
$$

where (a) follows from the Markov chain $(W_1, W_2, F_1, F_2) - (\widetilde{X}_1^n, \widetilde{X}_2^n) - (Y^n, Z^n)$, (b) follows since (V_1^n, V_2^n) determine $(F_{v_1}, W_{v_1}, F_{v_2}, W_{v_2})$, (c) follows because $(F_{v_1}, W_{v_1}, \widetilde{X}_1^n, \widetilde{X}_2^n)$ can reliably recover V_1^n by (25), and similarly because $(F_{v_2}, W_{v_2}, V_1^n, \widetilde{X}_1^n, \widetilde{X}_2^n)$ can reliably recover V_2^n by (26) both due to the Markov chain $(V_1^n, V_2^n) - (\widetilde{X}_1^n, \widetilde{X}_2^n) - Y^n$, (d) follows since (U_1^n, U_2^n) determine $(F_{u_1}, W_{u_1}, F_{u_2}, W_{u_2})$, (e) follows because $(F_{u_1}, W_{u_1}, V_1^n, V_2^n, \widetilde{X}_1^n, \widetilde{X}_2^n)$ can reliably recover U_1^n by (27) and the inequality $H(U_1|V_1, V_2, Y) \geq H(U_1|V_1, V_2, \widetilde{X}_1, \widetilde{X}_2^n)$ that can be proved similarly to (48) due to the Markov chain $U_1 - (V_1, V_2, \widetilde{X}_1, \widetilde{X}_2) - Y$. Similarly, $(F_{u_2}, W_{u_2}, V_1^n, V_2^n, U_1^n, \widetilde{X}_1^n, \widetilde{X}_2^n)$ can reliably recover U_2^n by (28) and the inequality $H(U_2|V_1, V_2, U_1, Y) \geq H(U_2|V_1, V_2, U_1, \widetilde{X}_1, \widetilde{X}_2)$ that can be proved by using the Markov chain $U_2 - (V_1, V_2, U_1, \widetilde{X}_1, \widetilde{X}_2) - Y$, and (f) follows because $(U_1^n, U_2^n, V_1^n, V_2^n, \widetilde{X}_1^n, \widetilde{X}_2^n)$ are i.i.d.

We remark that the terms in (50) are entirely similar to the terms in (47). One can show that all steps of the decodability analysis from [27, Section V-A] that is applied to (47) can be applied also to (50) by replacing X with $(\widetilde{X}_1, \widetilde{X}_2)$, so we obtain

$$
\begin{aligned}
&I(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n; W_1, W_2, F_1, F_2 | Z^n) \\
&\leq n[I(U_1, U_2; Z | V_1, V_2) - I(U_1, U_2; Y | V_1, V_2) + \epsilon]^- \\
&\quad + nI(U_1, U_2; \widetilde{X}_1, \widetilde{X}_2 | Z) + 5n\epsilon_n'. \qquad (51)
\end{aligned}
$$

We consider that the public indices (F_1, F_2) are generated uniformly at random and the encoders generate (V_1^n, U_1^n) and (V_2^n, U_2^n) according to $P_{V_1^n U_1^n V_2^n U_2^n | \widetilde{X}_1^n F_1 \widetilde{X}_2^n F_2}$ obtained from the binning scheme above. This procedure induces a joint probability distribution that is almost equal to $P_{V_1 V_2 U_1 U_2 \widetilde{X}_1 \widetilde{X}_2 X Y Z}$ fixed by (14) [26, Section 1.6]. Since the privacy and secrecy leakage metrics considered above are expectations over all possible realizations $F = f$, applying the selection lemma [28, Lemma 2.2], these results prove the achievability for Theorem 1 by choosing an $\epsilon > 0$ such that $\epsilon \to 0$ when $n \to \infty$. We remark that the achievable region is convexified by using a time-sharing random variable Q such that $P_{Q V_1 V_2} = P_Q P_{V_1|Q} P_{V_2|Q}$, required because of the $[\cdot]^-$ operation. □

B. Outer Bound Proof Sketch

Proof. Assume that for some $n \geq 1$ and $\delta_n > 0$, there exist two encoders and a decoder such that (2)-(7) are satisfied for some tuple $(R_{\mathrm{s}}, R_{\mathrm{w}_1}, R_{\mathrm{w},2}, R_{\ell,\mathrm{Dec}}, R_{\ell,\mathrm{Eve}})$. Let $V_{1,i} \triangleq (W_1, Y_{i+1}^n, Z^{i-1})$, $V_{2,i} \triangleq (W_2, Y_{i+1}^n, Z^{i-1})$, $U_{1,i} \triangleq (X^{i-1}, W_1, Y_{i+1}^n, Z^{i-1})$, and $U_{2,i} \triangleq (X^{i-1}, W_2, Y_{i+1}^n, Z^{i-1})$ that satisfy the Markov chains

$$V_{1,i} - U_{1,i} - \widetilde{X}_{1,i} - X_i - (\widetilde{X}_{2,i}, Y_i, Z_i) \qquad (52)$$

$$V_{2,i} - U_{2,i} - \widetilde{X}_{2,i} - X_i - (\widetilde{X}_{1,i}, Y_i, Z_i). \qquad (53)$$

Admissibility of $(\mathbf{U_1}, \mathbf{U_2})$: Define

$$n\epsilon_n = n\delta_n |\widetilde{\mathcal{X}}_1||\widetilde{\mathcal{X}}_2||\mathcal{Y}| + H_b(\delta_n) \qquad (54)$$

where $H_b(\delta) = -(1-\delta)\log(1-\delta) - \delta \log \delta$ is the binary entropy function such that $\epsilon_n \to 0$ if $\delta_n \to 0$. Using Fano's inequality and (2), we obtain

$$
\begin{aligned}
n\epsilon_n &\geq H(f^n | \widehat{f^n}) \overset{(a)}{=} H(f^n | \bar{f}^n) = \sum_{i=1}^n H(f_i | \bar{f}_i) \\
&\geq \sum_{i=1}^n H(f_i | \bar{f}^n) \overset{(b)}{\geq} \sum_{i=1}^n H(f_i | W_1, W_2, Y^n) \\
&\geq \sum_{i=1}^n H(f_i | W_1, W_2, Y^n, X^{i-1}, Z^{i-1}) \\
&\overset{(c)}{=} \sum_{i=1}^n H(f_i | W_1, W_2, Y_{i+1}^n, X^{i-1}, Z^{i-1}, Y_i) \\
&\overset{(d)}{=} \sum_{i=1}^n H(f_i | U_{1,i}, U_{2,i}, Y_i) \qquad (55)
\end{aligned}
$$

where (a) follows from [29, Lemma 2] that proves that when $n \to \infty$, there exists an i.i.d. random variable $\bar{f}^n$ that satisfies both $H(f^n|\widehat{f^n}) = H(f^n|\bar{f}^n)$ and the Markov chain $\widehat{f^n} - \bar{f}^n - (W_1, W_2, Y^n)$, (b) follows from the data processing inequality because of the Markov chain $f^n - (W_1, W_2, Y^n) - \bar{f}^n$ and permits randomized decoding, (c) follows from the Markov chain

$$Y^{i-1} - (X^{i-1}, Z^{i-1}, W_1, W_2, Y_i, Y_{i+1}^n) - f_i \qquad (56)$$

and (d) follows from the definitions of $U_{1,i}$ and $U_{2,i}$.

Public Message (Storage) Rates: We obtain

$$
\begin{aligned}
&n(R_{\mathrm{w}_1} + \delta_n) \overset{(a)}{\geq} \log |\mathcal{W}_1| \geq H(W_1|Y^n) - H(W_1|\widetilde{X}_1^n, Y^n) \\
&= H(\widetilde{X}_1^n | Y^n) - H(\widetilde{X}_1^n | W_1, Y^n)
\end{aligned}
$$

$$
\begin{aligned}
&= H(\widetilde{X}_1^n|Y^n) - \sum_{i=1}^{n} H(\widetilde{X}_{1,i}|\widetilde{X}_1^{i-1}, W_1, Y^n) \\
&\overset{(b)}{=} H(\widetilde{X}_1^n|Y^n) - \sum_{i=1}^{n} H(\widetilde{X}_{1,i}|\widetilde{X}_1^{i-1}, W_1, Y_{i+1}^n, Y_i) \\
&\overset{(c)}{\geq} H(\widetilde{X}_1^n|Y^n) - \sum_{i=1}^{n} H(\widetilde{X}_{1,i}|X^{i-1}, Z^{i-1}, W_1, Y_{i+1}^n, Y_i) \\
&\overset{(d)}{=} nH(\widetilde{X}_1|Y) - \sum_{i=1}^{n} H(\widetilde{X}_{1,i}|U_{1,i}, Y_i) = \sum_{i=1}^{n} I(U_{1,i}; \widetilde{X}_{1,i}|Y_i) \\
&\overset{(e)}{=} \sum_{i=1}^{n} [I(V_{1,i}; \widetilde{X}_{1,i}|Y_i) + I(U_{1,i}; \widetilde{X}_{1,i}|Y_i, V_{1,i})] \\
&= \sum_{i=1}^{n} \Big[I(V_{1,i}; \widetilde{X}_{1,i}, V_{2,i}|Y_i) - I(V_{1,i}; V_{2,i}|\widetilde{X}_{1,i}, Y_i) \\
&\qquad + I(U_{1,i}; \widetilde{X}_{1,i}, U_{2,i}|Y_i, V_{1,i}) \\
&\qquad - I(U_{1,i}; U_{2,i}|\widetilde{X}_{1,i}, Y_i, V_{1,i}) \Big] \\
&\geq \sum_{i=1}^{n} \Big[I(V_{1,i}; \widetilde{X}_{1,i}|Y_i, V_{2,i}) - I(V_{1,i}; V_{2,i}|\widetilde{X}_{1,i}, Y_i) \\
&\qquad + I(U_{1,i}; \widetilde{X}_{1,i}|Y_i, V_{1,i}, U_{2,i}) \\
&\qquad - I(U_{1,i}; U_{2,i}|\widetilde{X}_{1,i}, Y_i, V_{1,i}) \Big] \qquad (57)
\end{aligned}
$$

where (a) follows by (4), (b) follows from the Markov chain

$$Y^{i-1} - (\widetilde{X}_1^{i-1}, W_1, Y_{i+1}^n, Y_i) - \widetilde{X}_{1,i} \qquad (58)$$

(c) follows from the data processing inequality applied to the Markov chain

$$(X^{i-1}, Z^{i-1}) - (\widetilde{X}_1^{i-1}, W_1, Y_{i+1}^n, Y_i) - \widetilde{X}_{1,i} \qquad (59)$$

(d) follows from the definition of $U_{1,i}$, and (e) follows by (52). Similarly, one can show that we have

$$
\begin{aligned}
&n(R_{\mathrm{w}_2} + \delta_n) \\
&\geq \sum_{i=1}^{n} \Big[I(V_{2,i}; \widetilde{X}_{2,i}|Y_i, V_{1,i}) - I(V_{2,i}; V_{1,i}|\widetilde{X}_{2,i}, Y_i) \\
&\qquad + I(U_{2,i}; \widetilde{X}_{2,i}|Y_i, V_{2,i}, U_{1,i}) \\
&\qquad - I(U_{2,i}; U_{1,i}|\widetilde{X}_{2,i}, Y_i, V_{2,i}) \Big]. \qquad (60)
\end{aligned}
$$

Now we consider the sum-rate bound such that

$$
\begin{aligned}
&n(R_{\mathrm{w}_1} + \delta_n) + n(R_{\mathrm{w}_2} + \delta_n) \overset{(a)}{\geq} \log(|\mathcal{W}_1| \cdot |\mathcal{W}_2|) \\
&\geq H(W_1, W_2) \geq I(W_1, W_2; \widetilde{X}_1^n, \widetilde{X}_2^n) - I(W_1, W_2; Y^n) \\
&\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, Y_{i+1}^n) \\
&\qquad - I(W_1, W_2; Y_i|\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, Y_{i+1}^n) \Big] \\
&\overset{(c)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2, \widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, Y_{i+1}^n; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \\
&\qquad - I(W_1, W_2, \widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, Y_{i+1}^n; Y_i) \Big] \\
&\overset{(d)}{\geq} \sum_{i=1}^{n} \Big[I(W_1, W_2, X^{i-1}, Z^{i-1}, Y_{i+1}^n; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \\
&\qquad - I(W_1, W_2, X^{i-1}, Z^{i-1}, Y_{i+1}^n; Y_i) \Big] \\
&\overset{(e)}{=} \sum_{i=1}^{n} \Big[I(U_{1,i}, U_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}) - I(U_{1,i}, U_{2,i}; Y_i) \Big] \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(U_{1,i}, U_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i) \\
&\overset{(g)}{=} \sum_{i=1}^{n} \Big[I(U_{1,i}, U_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i, V_{1,i}, V_{2,i}) \\
&\qquad + I(V_{1,i}, V_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i) \Big] \\
&\overset{(h)}{=} \sum_{i=1}^{n} \Big[I(U_{1,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i, V_{1,i}, V_{2,i}) \\
&\qquad + I(U_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i, U_{1,i}, V_{2,i}) \\
&\qquad + I(V_{1,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i) \\
&\qquad + I(V_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}|Y_i, V_{1,i}) \Big] \\
&\geq \sum_{i=1}^{n} \Big[I(U_{1,i}; \widetilde{X}_{1,i}|Y_i, V_{1,i}, V_{2,i}) \\
&\qquad + I(U_{2,i}; \widetilde{X}_{2,i}|Y_i, U_{1,i}, V_{2,i}) \\
&\qquad + I(V_{1,i}; \widetilde{X}_{1,i}|Y_i) + I(V_{2,i}; \widetilde{X}_{2,i}|Y_i, V_{1,i}) \Big] \qquad (61)
\end{aligned}
$$

where (a) follows by (4) and (5), (b) follows from Csiszár's sum identity [30], (c) follows because $(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n)$ are i.i.d., (d) follows from the data processing inequality applied to the Markov chains

$$
\begin{aligned}
&(X^{i-1}, Z^{i-1}) - (\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, W_1, W_2, Y_{i+1}^n) - (\widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \\
&(\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}) - (X^{i-1}, Z^{i-1}, W_1, W_2, Y_{i+1}^n) - Y_i \qquad (62)
\end{aligned}
$$

(e) follows from the definitions of $U_{1,i}$ and $U_{2,i}$, (f) and (g) follow from the Markov chain

$$(V_{1,i}, V_{2,i}) - (U_{1,i}, U_{2,i}) - (\widetilde{X}_{1,i}, \widetilde{X}_{2,i}) - Y_i \qquad (63)$$

(h) follows from the Markov chain

$$V_{1,i} - (U_{1,i}, Y_i, V_{2,i}) - (U_{2,i}, \widetilde{X}_{1,i}, \widetilde{X}_{2,i}). \qquad (64)$$

Privacy Leakage to Decoder: We have

$$
\begin{aligned}
&n(R_{\ell,\mathrm{Dec}} + \delta_n) \overset{(a)}{\geq} H(W_1, W_2|Y^n) - H(W_1, W_2|X^n) \\
&\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; X_i|X^{i-1}, Y_{i+1}^n) \\
&\qquad - I(W_1, W_2; Y_i|Y_{i+1}^n, X^{i-1}) \Big] \\
&\overset{(c)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; X_i|X^{i-1}, Z^{i-1}, Y_{i+1}^n) \\
&\qquad - I(W_1, W_2; Y_i|Y_{i+1}^n, X^{i-1}, Z^{i-1}) \Big]
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(d)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2, X^{i-1}, Z^{i-1}, Y_{i+1}^n; X_i) \\
&\qquad - I(W_1, W_2, Y_{i+1}^n, X^{i-1}, Z^{i-1}; Y_i) \Big] \\
&\overset{(e)}{=} \sum_{i=1}^{n} \Big[I(U_{1,i}, U_{2,i}; X_i) - I(U_{1,i}, U_{2,i}; Y_i) \Big] \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(U_{1,i}, U_{2,i}; X_i | Y_i) \qquad (65)
\end{aligned}
$$

where (a) follows by (6) and from the Markov chain $(W_1, W_2) - X^n - Y^n$, (b) follows from Csiszár's sum identity, (c) follows from the Markov chain

$$
Z^{i-1} - (X^{i-1}, Y_{i+1}^n) - (X_i, Y_i, W_1, W_2) \qquad (66)
$$

(d) follows because (X^n, Y^n, Z^n) are i.i.d., (e) follows from the definitions of $U_{1,i}$ and $U_{2,i}$, and (f) follows from the Markov chain $(U_{1,i}, U_{2,i}) - X_i - Y_i$.

Privacy Leakage to Eve: We have

$$
\begin{aligned}
&n(R_{\ell,\text{Eve}} + \delta_n) \\
&\overset{(a)}{\geq} [H(W_1, W_2|Z^n) - H(W_1, W_2|Y^n)] \\
&\qquad + [H(W_1, W_2|Y^n) - H(W_1, W_2|X^n)] \\
&\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; Y_i | Y_{i+1}^n, Z^{i-1}) \\
&\qquad - I(W_1, W_2; Z_i | Z^{i-1}, Y_{i+1}^n) \Big] \\
&\quad + \sum_{i=1}^{n} \Big[I(W_1, W_2; X_i | X^{i-1}, Y_{i+1}^n) \\
&\qquad - I(W_1, W_2; Y_i | Y_{i+1}^n, X^{i-1}) \Big] \\
&\overset{(c)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; Y_i | Y_{i+1}^n, Z^{i-1}) \\
&\qquad - I(W_1, W_2; Z_i | Z^{i-1}, Y_{i+1}^n) \Big] \\
&\quad + \sum_{i=1}^{n} \Bigg[I(W_1, W_2; X_i | X^{i-1}, Y_{i+1}^n, Z^{i-1}) \\
&\qquad - I(W_1, W_2; Y_i | Y_{i+1}^n, X^{i-1}, Z^{i-1}) \Bigg] \\
&\overset{(d)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2, Y_{i+1}^n, Z^{i-1}; Y_i) \\
&\qquad - I(W_1, W_2, Z^{i-1}, Y_{i+1}^n; Z_i) \Big] \\
&\quad + \sum_{i=1}^{n} \Bigg[I(W_1, W_2, X^{i-1}, Y_{i+1}^n, Z^{i-1}; X_i) \\
&\qquad - I(W_1, W_2, Y_{i+1}^n, X^{i-1}, Z^{i-1}; Y_i) \Bigg] \\
&\overset{(e)}{=} \sum_{i=1}^{n} \Big[I(V_{1,i}, V_{2,i}; Y_i) - I(V_{1,i}, V_{2,i}; Z_i) \\
&\qquad + I(U_{1,i}, U_{2,i} V_{1,i}, V_{2,i}; X_i) \\
&\qquad - I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; Y_i) \Big] \\
&= \sum_{i=1}^{n} \Big[- I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; Z_i) \\
&\qquad + I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; X_i) \\
&\qquad + I(U_{1,i}, U_{2,i}; Z_i | V_{1,i}, V_{2,i}) \\
&\qquad - I(U_{1,i}, U_{2,i}; Y_i | V_{1,i}, V_{2,i}) \Big] \\
&\overset{(f)}{\geq} \sum_{i=1}^{n} \Bigg[I(U_{1,i}, U_{2,i}; X_i | Z_i) \\
&\qquad + \Big[I(U_{1,i}, U_{2,i}; Z_i | V_{1,i}, V_{2,i}) \\
&\qquad - I(U_{1,i}, U_{2,i}; Y_i | V_{1,i}, V_{2,i}) \Big]^- \Bigg] \qquad (67)
\end{aligned}
$$

where (a) follows by (7) and from the Markov chain $(W_1, W_2) - X^n - Z^n$, (b) follows from Csiszár's sum identity, (c) follows from the Markov chain in (66), (d) follows because (X^n, Y^n, Z^n) are i.i.d., (e) follows from the definitions of $V_{1,i}$, $V_{2,i}$, $U_{1,i}$ and $U_{2,i}$, and (f) follows from the Markov chain $(V_{1,i}, V_{2,i}) - (U_{1,i}, U_{2,i}) - X_i - Z_i$.

Secrecy Leakage (to Eve): We obtain

$$
\begin{aligned}
&n(R_{\text{s}} + \delta_n) \\
&\overset{(a)}{\geq} [H(W_1, W_2|Z^n) - H(W_1, W_2|Y^n)] \\
&\qquad + [H(W_1, W_2|Y^n) - H(W_1, W_2|\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n)] \\
&\overset{(b)}{=} \sum_{i=1}^{n} \Big[I(W_1, W_2; Y_i | Y_{i+1}^n, Z^{i-1}) \\
&\qquad - I(W_1, W_2; Z_i | Z^{i-1}, Y_{i+1}^n) + H(\widetilde{X}_{1,i}, \widetilde{X}_{2,i} | Y_i) \\
&\qquad - H(\widetilde{X}_{1,i}, \widetilde{X}_{2,i} | \widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, W_1, W_2, Y_{i+1}^n, Y_i) \Big] \\
&\overset{(c)}{\geq} \sum_{i=1}^{n} \Big[I(W_1, W_2, Y_{i+1}^n, Z^{i-1}; Y_i) \\
&\qquad - I(W_1, W_2, Z^{i-1}, Y_{i+1}^n; Z_i) + H(\widetilde{X}_{1,i}, \widetilde{X}_{2,i} | Y_i) \\
&\qquad - H(\widetilde{X}_{1,i}, \widetilde{X}_{2,i} | X^{i-1}, Z^{i-1}, W_1, W_2, Y_{i+1}^n, Y_i) \Big] \\
&\overset{(d)}{=} \sum_{i=1}^{n} \Big[I(V_{1,i}, V_{2,i}; Y_i) - I(V_{1,i}, V_{2,i}; Z_i) \\
&\qquad + I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i} | Y_i) \Big] \\
&\overset{(e)}{=} \sum_{i=1}^{n} \Big[I(V_{1,i}, V_{2,i}; Y_i) - I(V_{1,i}, V_{2,i}; Z_i) \\
&\qquad + I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \\
&\qquad - I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; Y_i) \Big]
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} \Big[-I(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}; Z_i) \\
&\qquad + I(U_{1,i}U_{2,i}, V_{1,i}, V_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \\
&\qquad + I(U_{1,i}, U_{2,i}; Z_i | V_{1,i}, V_{2,i}) \\
&\qquad - I(U_{1,i}, U_{2,i}; Y_i | V_{1,i}, V_{2,i}) \Big] \\
&\overset{(f)}{\geq} \sum_{i=1}^{n} \Bigg[I(U_{1,i}, U_{2,i}; \widetilde{X}_{1,i}, \widetilde{X}_{2,i} | Z_i) \\
&\qquad + \Big[I(U_{1,i}, U_{2,i}; Z_i | V_{1,i}, V_{2,i}) \\
&\qquad\qquad - I(U_{1,i}, U_{2,i}; Y_i | V_{1,i}, V_{2,i}) \Big]^{-} \Bigg] \qquad (68)
\end{aligned}
$$

where (a) follows by (3), (b) follows because $(\widetilde{X}_1^n, \widetilde{X}_2^n, Y^n)$ are i.i.d., and from Csiszár's sum identity and the Markov chain

$$Y^{i-1} - (\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, W_1, W_2, Y_{i+1}^n, Y_i) - (\widetilde{X}_{1,i}, \widetilde{X}_{2,i}) \quad (69)$$

(c) follows because (Y^n, Z^n) are i.i.d. and from the data processing inequality applied to the Markov chain

$$(X^{i-1}, Z^{i-1}) - (\widetilde{X}_1^{i-1}, \widetilde{X}_2^{i-1}, W_1, W_2, Y_{i+1}^n, Y_i) - (\widetilde{X}_{1,i}, \widetilde{X}_{1,i})$$

(d) follows from the definitions of $V_{1,i}$, $V_{2,i}$, $U_{1,i}$, and $U_{2,i}$, (e) follows from the Markov chain $(U_{1,i}, U_{2,i}, V_{1,i}, V_{2,i}) - (\widetilde{X}_{1,i}, \widetilde{X}_{2,i}) - Y_i$, and (f) follows from the Markov chain $(V_{1,i}, V_{2,i}) - (U_{1,i}, U_{2,i}) - (\widetilde{X}_{1,i}, \widetilde{X}_{2,i}) - Z_i$.

Introduce a uniformly distributed time-sharing random variable $Q \sim \text{Unif}[1:n]$ that is independent of other random variables, and define $X = X_Q$, $\widetilde{X}_1 = \widetilde{X}_{1,Q}$, $\widetilde{X}_2 = \widetilde{X}_{2,Q}$, $Y = Y_Q$, $Z = Z_Q$, $V_1 = V_{1,Q}$, $V_2 = V_{2,Q}$, $U_1 = (U_{1,Q}, Q)$, $U_2 = (U_{2,Q}, Q)$, and $f = f_Q$, so $(Q, V_1) - U_1 - \widetilde{X}_1 - X - (\widetilde{X}_2, Y, Z)$ and $(Q, V_2) - U_2 - \widetilde{X}_2 - X - (\widetilde{X}_1, Y, Z)$ form Markov chains. The proof of the outer bound follows by letting $\delta_n \to 0$.

Cardinality Bounds: We use the support lemma [30, Lemma 15.4] to prove the cardinality bounds and apply similar steps as in [17], [20], so we omit the proof. □

ACKNOWLEDGMENT

This work has been supported in part by the German Research Foundation (DFG) under the Grant SCHA 1944/9-1 and in part by the US National Science Foundation (NSF) under the Grant CCF 1955401.

REFERENCES

[1] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[2] J. B. Predd, S. B. Kulkarni, and H. V. Poor, "Distributed learning in wireless sensor networks," *IEEE Sign. Process. Mag.*, vol. 23, no. 4, pp. 56–69, July 2006.

[3] A. C. Yao, "Protocols for secure computations," in *IEEE Symp. Foundations Comp. Sci.*, Chicago, IL, Nov. 1982, pp. 160–164.

[4] ——, "How to generate and exchange secrets," in *IEEE Symp. Foundations Comp. Sci.*, Toronto, ON, Canada, Oct. 1986, pp. 162–167.

[5] 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.

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

[7] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

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

[9] 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, Aug. 2011.

[10] M. Sefidgaran and A. Tchamkerten, "Computing a function of correlated sources: A rate region," in *IEEE Int. Symp. Inf. Theory*, St. Petersburg, Russia, July-Aug. 2011, pp. 1856–1860.

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

[12] 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, Feb. 2012.

[13] S. Kannan and P. Viswanath, "Multi-session function computation and multicasting in undirected graphs," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 702–713, Mar. 2013.

[14] M. Goldenbaum, H. Boche, and H. V. Poor, "On secure computation over the binary modulo-2 adder multiple-access wiretap channel," in *IEEE Inf. Theory Workshop*, Cambridge, U.K., Sep. 2016, pp. 21–25.

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

[16] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *IEEE Inf. Theory Workshop*, Lake Tahoe, CA, Sep. 2007, pp. 442–447.

[17] W. Tu and L. Lai, "On function computation with privacy and secrecy constraints," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6716–6733, Oct. 2019.

[18] O. Günlü and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2872–2883, Nov. 2018.

[19] O. Günlü, "Key agreement with physical unclonable functions and biometric identifiers," Ph.D. dissertation, TU Munich, Germany, Nov. 2018, published by Dr.-Hut Verlag in Feb. 2019.

[20] O. Günlü, M. Bloch, and R. F. Schaefer, "Secure multi-function computation with private remote sources," June 2021, [Online]. Available: arxiv.org/abs/2106.09485.

[21] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A theoretical analysis of authentication, privacy, and reusability across secure biometric systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1825–1840, July 2012.

[22] O. Günlü, K. Kittichokechai, R. F. Schaefer, and G. Caire, "Controllable identifier measurements for private authentication with secret keys," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 1945–1959, Aug. 2018.

[23] O. Günlü, R. F. Schaefer, and G. Kramer, "Private authentication with physical identifiers through broadcast channel measurements," in *IEEE Inf. Theory Workshop*, Visby, Sweden, Aug. 2019, pp. 1–5.

[24] M. H. Yassaee, M. R. Aref, and A. Gohari, "Achievability proof via output statistics of random binning," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 6760–6786, Nov. 2014.

[25] T. Ericson and J. Körner, "Successive encoding of correlated sources," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 390–395, May 1983.

[26] M. Bloch, *Lecture Notes in Information-Theoretic Security*. Atlanta, GA: Georgia Inst. Technol., July 2018.

[27] O. Günlü, "Multi-entity and multi-enrollment key agreement with correlated noise," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1190–1202, 2021.

[28] M. Bloch and J. Barros, *Physical-layer Security*. Cambridge, U.K.: Cambridge University Press, 2011.

[29] O. Günlü, R. F. Schaefer, and H. V. Poor, "Biometric and physical identifiers with correlated noise for controllable private authentication," July 2020, [Online]. Available: arxiv.org/abs/2001.00847.

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