

Byzantine Multiple Access Channels—Part I: Reliable Communication

Neha Sangwan^{ID}, Mayank Bakshi^{ID}, Member, IEEE, Bikash Kumar Dey^{ID}, Member, IEEE,
and Vinod M. Prabhakaran^{ID}, Member, IEEE

Abstract—We study communication over a Multiple Access Channel (MAC) where users can possibly be adversarial. The receiver is unaware of the identity of the adversarial users (if any). When all users are non-adversarial, we want their messages to be decoded reliably. When a user behaves adversarially, we require that the honest users' messages be decoded reliably. An adversarial user can mount an attack by sending any input into the channel rather than following the protocol. It turns out that the 2-user MAC capacity region follows from the point-to-point Arbitrarily Varying Channel (AVC) capacity. For the 3-user MAC in which at most one user may be malicious, we characterize the capacity region for deterministic codes and randomized codes (where each user shares an independent random secret key with the receiver). These results are then generalized for the k -user MAC where the adversary may control all users in one out of a collection of given subsets.

Index Terms—Multiple access channel (MAC), arbitrarily varying channels (AVCs), byzantine adversary, symmetrizability, channel capacity, multiuser channels, information theory, security, channel models.

I. INTRODUCTION

A. Motivation and Setup

COMMUNICATION systems such as the wireless Internet-of-Things (IoTs), which consist of devices of varying security levels connected over a wireless network, pose new security challenges [2], [3]. Since, the devices share the same communication medium, a malicious¹ device may

Manuscript received 13 January 2023; revised 21 August 2023; accepted 9 November 2023. Date of publication 12 December 2023; date of current version 19 March 2024. The work of Neha Sangwan was supported in part by Department of Atomic Energy (DAE) under Project RTI4001 and in part by the Tata Consultancy Services (TCS) Foundation through the TCS Research Scholar Program. The work of Mayank Bakshi was supported in part by the Research Grants Council of the Hong Kong Special Administrative Region, China, under Grant GRF 14300617; and in part by the National Science Foundation under Grant CCF-2107526. The work of Bikash Kumar Dey was supported by the Bharti Centre for Communication, Indian Institute of Technology Bombay. The work of Vinod M. Prabhakaran was supported in part by DAE under Project RTI4001 and in part by Science and Engineering Research Board (SERB) under Project MTR/2020/000308. An earlier version of this paper was presented in part at the 2019 IEEE Information Theory Workshop [DOI: 10.1109/ITW44776.2019.8989065]. (Corresponding author: Neha Sangwan.)

Neha Sangwan and Vinod M. Prabhakaran are with the Tata Institute of Fundamental Research, Mumbai 400005, India (e-mail: nehasangwan010@gmail.com).

Mayank Bakshi is with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287 USA.

Bikash Kumar Dey is with the Indian Institute of Technology Bombay, Mumbai 400076, India.

Communicated by T. Koch, Associate Editor for Communications.

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TIT.2023.3341902>.

Digital Object Identifier 10.1109/TIT.2023.3341902

¹We use ‘malicious’ and ‘adversarial’ interchangeably.

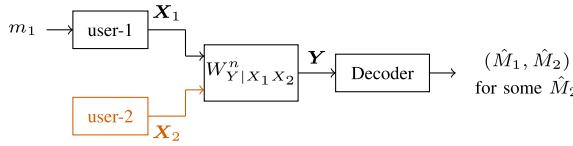
attempt to cause decoding errors for the honest device(s). This motivates the present problem. We study the uplink of a communication network in which users may behave maliciously.

Consider a Multiple Access Channel (MAC) with users who are potentially adversarial. An adversarial user may not follow the protocol and may choose its channel input maliciously to disrupt the communication of the other users. The receiver is unaware of whether any of the users is adversarial and the identity of the adversarial user(s) (if any). We call such a channel a “byzantine-MAC”. If all users are non-adversarial (*i.e.*, honest), we require that their messages be reliably decoded. However, if some of the users are adversarial, the decoder must correctly recover the messages of all the other (honest) users. Adversarial users have no side information about the messages of the honest users. We call this the problem of *reliable communication in a byzantine-MAC*.

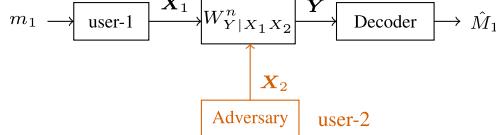
B. Related Works

The present model is different from other well-studied models involving non-byzantine users and adversaries, both *passive* and *active*. In all such models, the adversary is different from all the legitimate communicating parties and its identity is known to all parties.

For example, a wiretap channel [4] has a passive eavesdropper who gets a noisy version of the communication between the sender and the receiver. The goal is to ensure reliable and private (from the eavesdropper) communication from the sender to the receiver. On the other hand, in Arbitrarily Varying Channels (AVC) [5], [6] the adversary is active and controls the channel. The adversary can change the channel law for each channel use with the goal of jamming the communication between the sender and the receiver. Arbitrarily Varying Multiple Access Channels (AV-MAC) [7], [8], [9], [10], [11], [12], which consider a Multiple Access Channel (MAC) where the channel law is controlled by an adversary, have also been studied. Jahn [8] obtained the randomized coding capacity region where each user has independent randomness shared with the receiver. He also showed that this region is also the deterministic coding capacity region under average probability of error whenever the latter has a non-empty interior, a result along the lines of Ahlswede's dichotomy for the AVC [13]. Gubner [9] proved necessary conditions (non-symmetrizability conditions) for the deterministic coding capacity region to be non-empty. Ahlswede and Cai [10] showed that Gubner's necessary conditions are also sufficient for the deterministic coding capacity region to have a non-empty interior. More

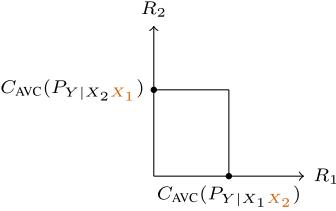


(a) A two-user byzantine-MAC where user-2 is malicious.



(b) A malicious user-2 can simulate an AVC from user-1 to the receiver where the input of user-2 is treated as the adversarial state. Thus, user-1 cannot communicate reliably at any rate above the capacity of this AVC. On the other hand, user-1 can achieve all the rates below the capacity of this AVC by using an appropriate AVC code.

Fig. 1. Capacity region of a two-user byzantine-MAC is given by the rectangular capacity region obtained by treating the channel from each user to the receiver as an AVC with the other user's input as the AVC state sequence.



(c) Capacity region of a two-user byzantine-MAC. $C_{AVC}(P_{Y|X_2S})$ is the capacity of AVC $P_{Y|X_2S}$ with input X_2 , state S and output Y .

recently, Pereg and Steinberg [11] obtained the capacity region for the AV-MAC with state constraints. Wiese and Boche [12] considered the two-user AV-MAC with conferencing encoders. In a recent work, Beemer, Graves, Kliewer, Kosut, and Yu [7] considered an authentication like model in a two-user AV-MAC, where all states, except one, are treated as adversarial states. Under adversarial states, the decoder's output can be a declaration of the presence of an adversary while also decoding at least one user's message.

In contrast to these works, the current model has *byzantine users*, *i.e.*, one of the legitimate users is potentially adversarial.

There are other works on models with *byzantine users* in the information theory literature, mostly in the setting of network coding. Byzantine attacks on the nodes and edges of networks have been studied under omniscient and weaker adversarial models in [14], [15], and [16], respectively. He and Yener [17] considered a Gaussian two-hop network with an eavesdropping and byzantine adversarial relay where the requirement is decoding the message with secrecy and byzantine attack detection. La and Anantharam [18] studied the MAC with strategic users modeled as a cooperative game with the objective of fairly allocating communication rate among the users.

For the byzantine-MAC, in a previous work [19], we looked at a weaker decoding guarantee than the present model, called *authenticated communication*. Under this weaker guarantee, the decoder must still reliably recover the messages when all the users are honest. However, if any user behaves adversarially, the decoder may either output the correct messages for the honest users or declare an error, *i.e.*, an adversary should not be able to cause an undetected erroneous output for the honest users. In a similar model of *communication with adversary identification* [20] in a byzantine-MAC with two users, a slightly stronger decoding guarantee was considered. Again, reliable decoding was required when all users are honest. In the presence of a malicious user, the decoder may either output a pair of messages out of which the message of the honest user is correct, or declare an error together with the identity of the malicious user. Both these models are different

from the present model, where we always require reliable decoding of the honest users' messages and the decoder may never declare an error².

C. Two-User byzantine-MAC

For the 2-user byzantine-MAC, consider the problem of reliable communication when any one of the users might be adversarial (though the decoder does not know *a priori* which, if any, of the users is adversarial). Clearly, each user can at least achieve the capacity of the AVC where the other user's input is treated as the channel state. Further, it is also easy to see that no higher rate is possible as, for the honest user's perspective, the other user, when adversarial, can behave exactly like an adversary in the AVC setup (see Figure 1(a) and (b)). Thus, the capacity region is the rectangular region defined by the AVC capacities of the two users' channels (Figure 1(c)), *i.e.*, there is no trade-off between the rates.³ Thus, the simplest non-trivial case is that of a 3-user byzantine-MAC with at most one adversarial user.

D. Three-User byzantine-MAC With at Most One Adversary

It turns out that all the key ideas can be presented in the relatively simpler setting of a 3-user byzantine-MAC (Figure 2) with at most one adversarial user. The general results then build on this. For this model, we characterize the capacity region under randomized coding where each user shares independent secret keys with the decoder, and deterministic coding with an average probability of error criterion.

²Journal versions of [19] and [20] are in preparation. Together with the present paper these constitute our multi-part study of Byzantine MACs encompassing various decoding requirements.

³This observation holds true under deterministic coding, stochastic encoding (where the encoders have private randomness), and randomized coding settings under both maximum and average probabilities of error. A similar observation can be made for a k -user byzantine-MAC where up to $k-1$ users may adversarially collude.

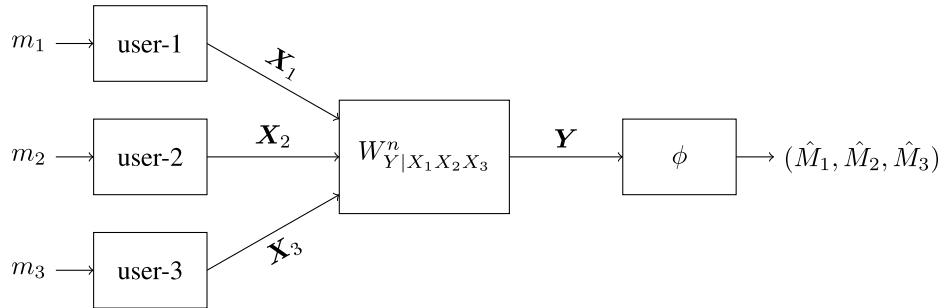


Fig. 2. Byzantine-MAC: At most one user may be adversarial. Reliable decoding of the messages of all honest users is required. Clearly, no decoding guarantees are given for an adversarial user.

1) *Randomized Coding*: Consider a three-user byzantine-MAC in which each user shares independent randomness with the decoder which is unknown to the other users. Notice that similar to the two-user byzantine-MAC where a malicious user could induce an AVC from the honest user to the receiver, in a three-user byzantine-MAC, a malicious user- i , $i \in \{1, 2, 3\}$ can induce a two-user AV-MAC $W^{(i)}$ from the honest users $\{1, 2, 3\} \setminus \{i\}$ to the receiver, where the input of the malicious user is treated as the adversarially chosen state sequence. For instance, if a rate triple (R_1, R_2, R_3) is achievable for the byzantine-MAC, then the rate pair (R_1, R_2) is also be achievable over the two-user AV-MAC $W^{(3)}$.⁴ We use this intuition to show the converse of the randomized coding capacity region (Theorem 3). We show the achievability by using a randomized code (from [8])⁵ for the two-user AV-MAC $W^{(i)}$, $i \in \{1, 2, 3\}$ and using random hashes for each message, generated using the independent shared randomness. See Section III-B2 for a sketch of achievability and Section IV-B for a detailed proof of achievability and converse.

2) *Deterministic Coding*: For deterministic coding, before discussing the capacity region, let us consider the following question: in which channels can all users *communicate reliably*?

In the AVC literature, the channels over which reliable communication is infeasible are called *symmetrizable channels* [21], [22]. In a symmetrizable AVC, the adversary can mount an attack which introduces a spurious message that can be confused with the actual message, resulting in a non-vanishing probability of error.

To answer the question, we first recall that a malicious user- i , $i \in \{1, 2, 3\}$, in a three-user byzantine-MAC, can induce a two-user AV-MAC $W^{(i)}$ formed by treating user- i 's input as an adversarially chosen state and the inputs of other two users as the inputs of legitimate users in the two-user AV-MAC. Thus, we inherit the symmetrizability conditions [9, Definition 3.1-3.3] from the three AV-MAC $W^{(1)}$, $W^{(2)}$ and $W^{(3)}$. We show that, in addition to the symmetrizability conditions inherited from the AV-MAC, fully

⁴In fact, a stronger necessary condition follows by noting that the encoder of each user must not depend on the knowledge of which user, if any, is the adversary. Thus, as in compound channels, the same code should work for $W^{(i)}$, $i \in \{1, 2, 3\}$. We use this observation in our converse arguments.

⁵Note that similar to the current model, in the AV-MAC model of [8], users share independent randomness with the decoder.

characterizing the feasibility of reliable communication of a 3-user byzantine-MAC requires three additional symmetrizability conditions (Eq. (8)). Roughly speaking, each of these conditions reflect whether or not an adversarial user at a node k can attack in a manner that is also consistent with an adversarial user at a node $j \neq k$ while resulting in a decoding ambiguity about the remaining user's message (see Figure 7). Example 1 (page 10) shows that the new symmetrizability conditions are not redundant given the symmetrizability conditions inherited from the two-user AV-MAC.

We characterize the deterministic coding capacity region under the average error criterion for most channels.⁶ There are two different approaches towards showing the achievability for the AVC using deterministic codes. We show achievability for the 3-user byzantine-MAC using both approaches and show a more general result for k -user byzantine-MAC using one of them.

a) *First approach*: The first approach uses a *randomness reduction* argument of Ahlswede [13] (and its extension for AV-MAC by Jahn [8]). He showed that given a randomized code of achievable rate R and block-length n , there exists another randomized code of achievable rate R which requires only $O(\log n)$ bits of randomness. This small amount of shared randomness can be established using deterministic codes. This shows the surprising fact that when the deterministic capacity is positive (which is the case for non-symmetrizable channels), it is in fact equal to the randomized coding capacity. Thus, to show achievability under deterministic codes, it suffices to show that all non-symmetrizable channels admit positive rates. Ahlswede and Cai in [10] took this route for the achievability proof of the two-user AV-MAC. For byzantine-MACs, we may follow a similar recipe (in fact, we do this for the general k -user byzantine-MAC). We show a *randomness reduction* argument along the lines of Jahn [8] and Ahlswede [13] (see Appendix V). With this and the randomized coding scheme discussed above (Section I-D1), all that remains is to show that in a non-symmetrizable byzantine-MAC, all users can transmit at positive rates using deterministic coding. The main difference from [10] in showing this, is that the code should

⁶Our characterization for deterministic codes is incomplete for channels in which some, but not all users are symmetrizable (for an appropriate notion of symmetrizability for a 3-user byzantine-MAC). See remark 1. We only study average probability of error under deterministic coding since the capacity under maximum probability of error remains open for multiple access channels (even with non-byzantine users) [23].

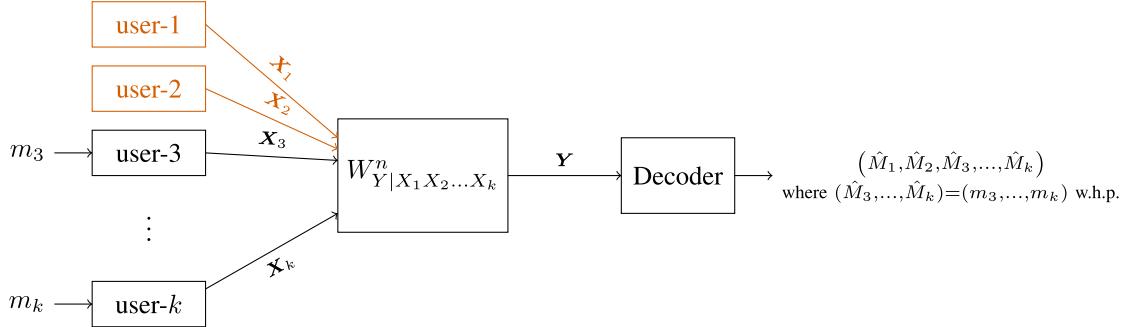


Fig. 3. Consider a k -user byzantine-MAC where the set containing users 1 and 2 belongs to the adversary structure. The figure depicts the case when users 1 and 2 deviate from the protocol under the control of an adversary. Then we require reliable decoding of the messages of all the honest users, *i.e.*, users 3 to k .

be able to handle any user behaving maliciously. Please see Section V for details.

b) *Second approach:* The second approach is a direct argument based on the method of types which establishes a deterministic code. The technique does not rely on the achievability of the randomized coding capacity. For the (point-to-point) AVC, Csiszár and Narayan [22] established the deterministic coding capacity using such an approach. Their achievability proof is based on a concentration result [22, Lemma A1]. A similar approach for multi-user channels (e.g. AV-MAC, byzantine-MAC etc.) requires extending this concentration result. We specialize the concentration result in [24, Theorem 2.1] to obtain just such an extension (Lemma 4 on page 13). This allows us to directly achieve all rate triples in the capacity region of a non-symmetrizable three-user byzantine-MAC (see Section IV-A). Our technique can also be used to obtain the deterministic coding capacity region of a two-user AV-MAC directly. We believe that this technique may have applications in other multi-user deterministic coding settings for adversarial channels and may be of independent interest.

E. k -User byzantine-MAC

In Section V, we consider a general k -user byzantine-MAC in which an adversary may control all users in any one of a set of subsets of users, called an *adversary structure*⁷ (see Fig. 3). The receiver is unaware which of these subsets the adversary controls. We provide a general symmetrization condition for the k -user byzantine-MACs. On the achievability side, we take the first achievability approach described above (see Section I-D2.a) and show a *randomness reduction* argument along the lines of Jahn [8] and Ahlswede [13]. We then show that as long as the given byzantine-MAC is non-symmetrizable, *i.e.*, none of the symmetrization conditions hold, the deterministic coding capacity region has a non-empty interior, in other words, all users can communicate at positive rates. Finally, we characterize the randomized coding capacity region using the same ideas as that for the three-user case. For the k -user byzantine-MAC, we do not pursue a direct proof

⁷The term ‘adversary structure’ is borrowed from cryptography. An adversary structure is a collection of subsets of users. The adversary may control all the users in any one of these subsets and use them to mount an attack (see, e.g., [25], [26], [27]).

using the second achievability approach described above (in Section I-D2.b) as it appears to be cumbersome.

F. Summary of Contributions

- We introduce the model of reliable communication in a byzantine-MAC, where malicious users may deviate from the prescribed protocol. The model requires that decoded messages should be correct for the honest users with high probability.
- We completely characterize the capacity region under both deterministic codes (with an average probability of error criterion) and randomized codes for any k -user byzantine-MAC.
- We also provide an alternate direct achievability for the 3-user byzantine-MAC, in the spirit of [22], where the achievability is based on a recent concentration result. This technique can be used to obtain a similar direct achievability for the 2-user AV-MAC (see Section I-D2.b) and may be of independent interest.

G. Outline

The system model and main results for the 3-user byzantine-MAC are given in Section III (Page 5). This section also contains the proof sketches. The main proofs of the results in Section III are given in Section IV (page 12). Others are deferred to the appendices. Section V presents the k -user byzantine-MAC model and gives main results. All the proofs of theorems in this section are given in the appendices.

II. NOTATION

Random variables are denoted by capital letters (possibly indexed) like X_1, X_2, X_3, Y , etc. The corresponding alphabets are denoted by calligraphic letters in the same format, for example, the random variable X_1 has alphabet \mathcal{X}_1 . Its n -product set is denoted by \mathcal{X}_1^n . We use bold faced letters to denote n -length vectors, for example, \mathbf{x} denotes a vector in \mathcal{X}^n and \mathbf{X} denotes a random vector taking values in \mathcal{X}^n . For a random variable X , we denote its distribution by P_X and use the notation $X \sim P_X$ to indicate this. For an alphabet \mathcal{X} , let $\mathcal{P}_{\mathcal{X}}^n$ denote the set of all empirical distributions of n length strings from \mathcal{X}^n . For a random variable $X \sim P_X$ such that $P_X \in \mathcal{P}_{\mathcal{X}}^n$, let T_X^n be the set of all n -length strings

with empirical distribution P_X . For $\mathbf{x} \in \mathcal{X}^n$, the statement $\mathbf{x} \in T_X^n$ defines P_X as the empirical distribution of \mathbf{x} and a random variable $X \sim P_X$. We denote a k -user multiple access channel by $W_{Y|X_1X_2\dots X_k}$ (or W for short) and its n -fold memoryless version by $W_{Y|X_1X_2\dots X_k}^n$ (or W^n for short). For a set \mathcal{S} , $2^{\mathcal{S}}$ denotes its power set, \mathcal{S}^c denotes its complement and $\text{int}(\mathcal{S})$ denotes its interior. A uniform distribution on any set \mathcal{S} is denoted by $\text{Unif}(\mathcal{S})$. For any n , the set $\{1, 2, \dots, n\}$ will be denoted by $[1 : n]$. We will use the acronyms ‘w.h.p.’ to mean ‘with high probability’. For any real number A , we use $|A|^+$ to mean A if $A \geq 0$. Otherwise, $|A|^+ = 0$.

The following notation will be used in Section V. For any sets \mathcal{S}_i , $i \in [1 : k]$ and for $\mathcal{B} \subseteq [1 : k]$, $\mathcal{S}_{\mathcal{B}}$ denotes the product set $\times_{i \in \mathcal{B}} \mathcal{S}_i$. The tuple $(s_i \in \mathcal{S}_i : i \in [1 : k])$ will be denoted by $s_{[1:k]} \in \mathcal{S}_{[1:k]}$ and when restricted to \mathcal{B} , we write $s_{\mathcal{B}} \in \mathcal{S}_{\mathcal{B}}$. The notation $g_{\mathcal{B}}(s_{\mathcal{B}})$ denotes $(g_i(s_i) : i \in \mathcal{B})$ for function g_i defined on \mathcal{S}_i , $i \in [1 : k]$.

III. THE THREE USER BYZANTINE-MAC WITH AT MOST ONE ADVERSARY

A. System Model

Consider the 3-user byzantine-MAC setup shown in Fig. 2. The memoryless channel $W_{Y|X_1X_2X_3}$ has input alphabets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3$, and output alphabet \mathcal{Y} .

Definition 1 (Deterministic Code): An (N_1, N_2, N_3, n) deterministic code for the byzantine-MAC $W_{Y|X_1X_2X_3}$ consists of the following:

- (i) three message sets, $\mathcal{M}_i = \{1, \dots, N_i\}$, $i = 1, 2, 3$,
- (ii) three encoders, $f_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$, $i = 1, 2, 3$, and
- (iii) a decoder, $\phi : \mathcal{Y}^n \rightarrow \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$.

We define the average probability of error P_e as the maximum of average error probabilities under four different scenarios, one corresponding to all users being honest and three corresponding to exactly one user being adversarial. Let $(\hat{M}_1, \hat{M}_2, \hat{M}_3) = \phi(Y^n)$.

$$P_e(f_1, f_2, f_3, \phi) \stackrel{\text{def}}{=} \max\{P_{e,0}, P_{e,1}, P_{e,2}, P_{e,3}\},$$

where the terms on the right-hand side are defined below. Note that our notation suppresses their dependence on the code. $P_{e,0}$ is the average probability of error when none of the users are adversarial,

$$P_{e,0} \stackrel{\text{def}}{=} \frac{1}{N_1 N_2 N_3} \sum_{(m_1, m_2, m_3) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3} e_0(m_1, m_2, m_3),$$

where

$$e_0(m_1, m_2, m_3) = \mathbb{P}((\hat{M}_1, \hat{M}_2, \hat{M}_3) \neq (m_1, m_2, m_3) \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)).$$

$P_{e,i}$, $i = 1, 2, 3$ is the average error probability under worst case deterministic attacks when user- i is adversarial. $P_{e,1}$ is as below. $P_{e,2}, P_{e,3}$ are defined similarly.

$$P_{e,1} \stackrel{\text{def}}{=} \max_{\mathbf{x}_1 \in \mathcal{X}_1^n} \frac{1}{N_2 N_3} \sum_{(m_2, m_3) \in \mathcal{M}_2 \times \mathcal{M}_3} e_1(\mathbf{x}_1, m_2, m_3),$$

where

$$e_1(\mathbf{x}_1, m_2, m_3) = \mathbb{P}((\hat{M}_2, \hat{M}_3) \neq (m_2, m_3) \mid \mathbf{X}_1 = \mathbf{x}_1, \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)). \quad (1)$$

We emphasize that

- a) the decoder is unaware of whether any of the users is adversarial and the identity of the adversarial user (if any).
- b) the adversary knows the encoders and the decoder, but is unaware of the messages transmitted by the other (non-adversarial) users.⁸

Note that it is sufficient to define $P_{e,i}$ under deterministic attacks by the adversarial user. To see this, consider the setting where user-1 is adversarial. Then, under any randomized attack $\tilde{\mathbf{X}}_1 \sim Q$ for any distribution Q on \mathcal{X}_1^n ,

$$\begin{aligned} & \mathbb{E}_Q \left[\frac{1}{N_2 N_3} \sum_{m_2, m_3} \mathbb{P}((\hat{M}_2, \hat{M}_3) \neq (m_2, m_3) \mid \mathbf{X}_1 = \tilde{\mathbf{X}}_1, \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \right] \\ &= \sum_{\mathbf{x}_1 \in \mathcal{X}_1^n} Q(\mathbf{x}_1) \frac{1}{N_2 N_3} \sum_{m_2, m_3} \mathbb{P}((\hat{M}_2, \hat{M}_3) \neq (m_2, m_3) \mid \mathbf{X}_1 = \mathbf{x}_1, \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \\ &\leq \sum_{\mathbf{x}_1 \in \mathcal{X}_1^n} Q(\mathbf{x}_1) P_{e,1} \\ &= P_{e,1}. \end{aligned} \quad (2)$$

In other words, the probability of error is maximized when the adversarial user selects a deterministic attack vector (that depends only on the channel and the deterministic code used). We also note that

$$P_{e,0} \leq P_{e,1} + P_{e,2} + P_{e,3}. \quad (3)$$

This is because

$$\begin{aligned} P_{e,0} &= \frac{1}{N_1 N_2 N_3} \sum_{m_1, m_2, m_3} \mathbb{P}((\hat{M}_1, \hat{M}_2, \hat{M}_3) \neq (m_1, m_2, m_3) \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \\ &= \frac{1}{N_1 N_2 N_3} \sum_{m_1, m_2, m_3} \mathbb{P}(\{(\hat{M}_1, \hat{M}_2) \neq (m_1, m_2)\} \cup \{(\hat{M}_2, \hat{M}_3) \neq (m_2, m_3)\} \cup \{(\hat{M}_1, \hat{M}_3) \neq (m_1, m_3)\} \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \\ &\leq \frac{1}{N_1 N_2 N_3} \sum_{m_1, m_2, m_3} \left\{ \mathbb{P}(\{(\hat{M}_1, \hat{M}_2) \neq (m_1, m_2)\} \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \right. \\ &\quad \left. + \mathbb{P}(\{(\hat{M}_2, \hat{M}_3) \neq (m_2, m_3)\} \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \right. \\ &\quad \left. + \mathbb{P}(\{(\hat{M}_1, \hat{M}_3) \neq (m_1, m_3)\} \mid \mathbf{X}_1 = f_1(m_1), \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)) \right\} \end{aligned}$$

⁸Recall that at most one user is adversarial.

$$\begin{aligned}
& + \mathbb{P}(\{(\hat{M}_1, \hat{M}_3) \neq (m_1, m_3)\} \mid \mathbf{X}_1 = f_1(m_1), \\
& \mathbf{X}_2 = f_2(m_2), \mathbf{X}_3 = f_3(m_3)\} \\
\leq & P_{e,1} + P_{e,2} + P_{e,3}.
\end{aligned}$$

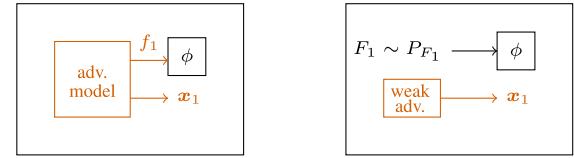
Definition 2 (Achievable Rate Triple and the Deterministic Coding Capacity Region): We say a rate triple (R_1, R_2, R_3) is *achievable* if there is a sequence of $(\lfloor 2^{nR_1} \rfloor, \lfloor 2^{nR_2} \rfloor, \lfloor 2^{nR_3} \rfloor, n)$ codes $(f_1^{(n)}, f_2^{(n)}, f_3^{(n)}, \phi^{(n)})$ for $n = 1, 2, \dots$ such that $\lim_{n \rightarrow \infty} P_e(f_1^{(n)}, f_2^{(n)}, f_3^{(n)}, \phi^{(n)}) \rightarrow 0$. The *deterministic coding capacity region* $\mathcal{R}_{\text{deterministic}}$ is the closure of the set of all achievable rate triples.

Definition 3 (Randomized Code): An (N_1, N_2, N_3, n) randomized code for the byzantine-MAC $W_{Y|X_1 X_2 X_3}$ consists of the following:

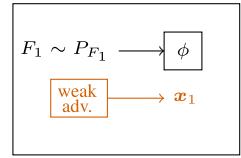
- (i) three message sets, $\mathcal{M}_i = \{1, \dots, N_i\}$, $i = 1, 2, 3$,
- (ii) three *independent* randomized encoders, $F_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$ where $F_i \sim P_{F_i}$ takes values in $\mathcal{F}_i \subseteq \{g : \mathcal{M}_i \rightarrow \mathcal{X}_i^n\}$, $i = 1, 2, 3$ and
- (iii) a decoder, $\phi : \mathcal{Y}^n \times \mathcal{F}_1 \times \mathcal{F}_2 \times \mathcal{F}_3 \rightarrow \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$ where $\phi(\mathbf{y}, F_1, F_2, F_3) = (\phi_1(\mathbf{y}, F_1, F_2, F_3), \phi_2(\mathbf{y}, F_1, F_2, F_3), \phi_3(\mathbf{y}, F_1, F_2, F_3))$ for some functions $\phi_i : \mathcal{Y}^n \times \mathcal{F}_1 \times \mathcal{F}_2 \times \mathcal{F}_3 \rightarrow \mathcal{M}_i$, $i = 1, 2, 3$.

In other words, a randomized code consists of *independent* random encoding maps F_1, F_2, F_3 and a decoder ϕ (which takes F_1, F_2, F_3 also as inputs), *i.e.*, the encoders randomize independently of each other and their randomization is available to the decoder. This is similar to the randomized code of Jahn [8] for 2-user AV-MACs. Notice that the decoder is a randomized decoder since the decoding function ϕ takes the random encoding maps F_1, F_2, F_3 as inputs.⁹ We emphasize that each byzantine user is unaware of the encoding maps of the other users. We also assume that the (byzantine) user- i samples its encoder F_i which is then made available to the decoder. Notice that the decoder ϕ is a function which maps the channel output as well as the random encoding maps to the decoded messages. This allows the adversarial user to adversarially choose its encoding map (in addition to its channel input) as part of its attack and thus attempt to influence the decoding. This means that an adversarial user i may choose $\mathbf{x}_i \in \mathcal{X}_i^n$ as input to the channel and any $f_i \in \mathcal{F}_i$ as the encoding map. This is shown in Fig. 4a. We denote the *randomized coding capacity region* by $\mathcal{R}_{\text{random}}$. We also consider another adversarial model, called the *weak* adversary. An adversary is a *weak* adversary if it does not have access to its own random encoding map when choosing its input vector, that is, the random encoding map F_i is sampled according to P_{F_i} and the adversarial input to the

⁹Any additional private randomness at the decoder can be subsumed as part of the randomness shared with each encoder in a slightly more general definition of randomized code (*i.e.*, a slight generalization of Definition 3) for which our converse in Section IV-B continues to hold. In this generalization, the users first sample (F_i, \mathbf{B}_i) ; $i = 1, 2, 3$ where \mathbf{B}_i are uniform bit strings, independent of F_i . Now, any additional private randomness at the decoder may be thought of as a bit string \mathbf{D} which is XOR of $\mathbf{B}_1, \mathbf{B}_2$ and \mathbf{B}_3 . Even, when one of the users, say user i , maliciously chooses \mathbf{B}_i , note that \mathbf{D} remains uniform and unknown to user i .



(a) An adversarial user-1 chooses an encoder map $f_1 \in \mathcal{F}_1$ and an input vector $\mathbf{x}_1 \in \mathcal{X}_1$ together.



(b) User-1 as a weak adversary sends a malicious input \mathbf{x}_1 independent and unaware of the choice of random encoder $F_1 \sim P_{F_1}$.

Fig. 4. A figure depicting various adversary models for randomized coding when user-1 is malicious.

channel \mathbf{x}_i is chosen independent of F_i (see Fig. 4b).¹⁰ We denote the corresponding randomized coding capacity region by $\mathcal{R}_{\text{random}}$. We show converse for the weak adversary. Clearly, $\mathcal{R}_{\text{random}} \subseteq \mathcal{R}_{\text{random}}$. Thus, a converse bound on $\mathcal{R}_{\text{random}}$ is also a converse bound on $\mathcal{R}_{\text{random}}$.

Analogous to the deterministic case, the average probability of error P_e^{rand} is defined as

$$P_e^{\text{rand}}(P_{F_1}, P_{F_2}, P_{F_3}, \phi) \stackrel{\text{def}}{=} \max\{P_{e,0}^{\text{rand}}, P_{e,1}^{\text{rand}}, P_{e,2}^{\text{rand}}, P_{e,3}^{\text{rand}}\},$$

where

$$P_{e,0}^{\text{rand}} \stackrel{\text{def}}{=} \frac{1}{N_1 N_2 N_3} \sum_{m_1, m_2, m_3} e_0^{\text{rand}}(m_1, m_2, m_3),$$

with

$$e_0^{\text{rand}}(m_1, m_2, m_3) = \mathbb{P}(\phi(Y^n, F_1, F_2, F_3) \neq (m_1, m_2, m_3) \mid \mathbf{X}_1 = F_1(m_1), \mathbf{X}_2 = F_2(m_2), \mathbf{X}_3 = F_3(m_3)).$$

The probability is over independent $F_i \sim P_{F_i}$, $i = 1, 2, 3$ and the randomness in the channel. $P_{e,1}^{\text{rand}}$ is as below, $P_{e,2}^{\text{rand}}, P_{e,3}^{\text{rand}}$ are defined similarly.

$$P_{e,1}^{\text{rand}} \stackrel{\text{def}}{=} \max_{\mathbf{x}_1 \in \mathcal{X}^n, f_1 \in \mathcal{F}_1} \frac{1}{N_2 N_3} \sum_{m_2, m_3} e_{f_1}(\mathbf{x}_1, m_2, m_3), \quad (4)$$

where

$$e_{f_1}(\mathbf{x}_1, m_2, m_3) = \mathbb{P}((\phi_2(\mathbf{Y}, f_1, F_2, F_3), \phi_3(\mathbf{Y}, f_1, F_2, F_3)) \neq (m_2, m_3) \mid \mathbf{X}_1 = \mathbf{x}_1, \mathbf{X}_2 = F_2(m_2), \mathbf{X}_3 = F_3(m_3)).$$

The probability is over independent $F_i \sim P_{F_i}$, $i = 2, 3$ and the channel. Restricting the attacks to deterministic attacks is without loss of generality along the lines of (2).

We define achievable rate triples and capacity region for randomized codes in a similar manner as the deterministic case.¹¹

¹⁰An intermediate model is the one where the adversary knows the random encoding map but does not have control over it. That is, for a malicious user i , $F_i \sim P_{F_i}$ and the input to the channel \mathbf{x}_i can be chosen as a function of F_i . In the proof of Theorem 3, the achievability is proved for the default adversary (who is stronger) while the converse is proved for the weak adversary. Hence, the capacity region for this intermediate model is the same as in Theorem 3.

¹¹Along the lines of [28, Problem 12.6 (b)], one can show that for randomized codes, the capacity region will remain unchanged for maximum and average probabilities of error criteria. Hence we only consider the average error criterion here.

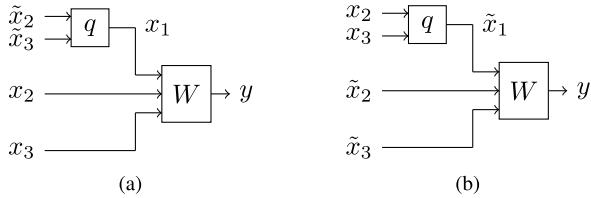


Fig. 5. We say $W_{Y|X_1X_2X_3}$ is $\mathcal{X}_2 \times \mathcal{X}_3$ -symmetrizable by \mathcal{X}_1 if, for each $(x_2, \tilde{x}_2, x_3, \tilde{x}_3)$, the conditional output distributions in the two cases above are the same. Thus, the receiver is unable to tell whether users 2 and 3 are sending (x_2, x_3) or $(\tilde{x}_2, \tilde{x}_3)$.

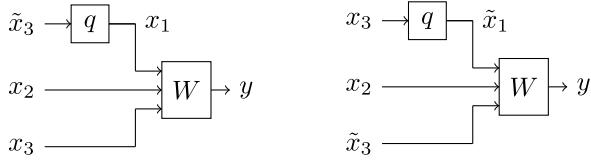


Fig. 6. We say $W_{Y|X_1X_2X_3}$ is $\mathcal{X}_3|\mathcal{X}_2$ -symmetrizable by \mathcal{X}_1 if, for each (x_2, x_3, \tilde{x}_3) , the conditional output distributions in the two cases above are the same. The receiver is unable to tell whether user-3 is sending x_3 or \tilde{x}_3 .

Definition 4 (Achievable Rate Triple and Randomized Coding Capacity Regions): We say a rate triple (R_1, R_2, R_3) is *achievable*, if there is a sequence of $(\lfloor 2^{nR_1} \rfloor, \lfloor 2^{nR_2} \rfloor, \lfloor 2^{nR_3} \rfloor, n)$ codes $\{F_1^{(n)}, F_2^{(n)}, F_3^{(n)}, \phi^{(n)}\}_{n=1}^{\infty}$ such that $\lim_{n \rightarrow \infty} P_e^{\text{rand}}(P_{F_1^{(n)}}, P_{F_2^{(n)}}, P_{F_3^{(n)}}, \phi^{(n)}) \rightarrow 0$. The *randomized coding capacity region* $\mathcal{R}_{\text{random}}$ is the closure of the set of all achievable rate triples.

The probability of error P_e^{weak} and the capacity region $\mathcal{R}_{\text{weak}}$ for randomized codes with a weak adversary are defined by replacing $P_{e,i}^{\text{rand}}$ with $P_{e,i}^{\text{weak}}$, $i = 1, 2, 3$ in the definition of $P_e^{\text{rand}}(P_{F_1}, P_{F_2}, P_{F_3}, \phi)$, where

$$P_{e,1}^{\text{weak}} \stackrel{\text{def}}{=} \max_{\mathbf{x}_1 \in \mathcal{X}^n} \frac{1}{N_2 N_3} \sum_{m_2, m_3} e_1^{\text{weak}}(\mathbf{x}_1, m_2, m_3), \quad (5)$$

where

$$e_1^{\text{weak}}(\mathbf{x}_1, m_2, m_3) = \mathbb{P}((\phi_2(\mathbf{Y}, F_1, F_2, F_3), \phi_3(\mathbf{Y}, F_1, F_2, F_3)) \neq (m_2, m_3) \mid \mathbf{X}_1 = \mathbf{x}_1, \mathbf{X}_2 = F_2(m_2), \mathbf{X}_3 = F_3(m_3)).$$

The probability is over independent $F_i \sim P_{F_i}$, $i = 1, 2, 3$ and the channel. $P_{e,2}^{\text{weak}}$ and $P_{e,3}^{\text{weak}}$ are defined similarly.

B. Main Results

1) Deterministic Coding Capacity Region: We first present our results for the three user byzantine-MAC with at most one adversary under deterministic coding. Analogous to the notion of symmetrizable [10], [22] in the AVC and AV-MAC literature, we give conditions under which at least one user cannot communicate with positive rate.

a) Symmetrizable conditions:

Definition 5: Let (i, j, k) be some permutation of $(1, 2, 3)$. We define three symmetrizable conditions for $W_{Y|X_1X_2X_3}$ (See Fig. 5-7).

1) We say that $W_{Y|X_1X_2X_3}$ is $\mathcal{X}_j \times \mathcal{X}_k$ -symmetrizable by \mathcal{X}_i if for some distribution $q(x_i|x_j, x_k)$

$$\sum_{x_i} q(x_i|\tilde{x}_j, \tilde{x}_k) W_{Y|X_i X_j X_k}(y|x_i, x_j, x_k)$$

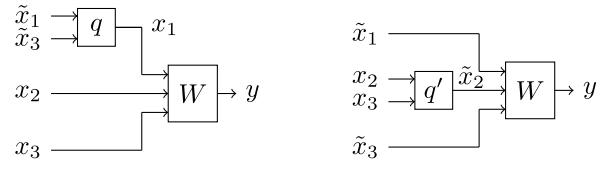


Fig. 7. We say $W_{Y|X_1X_2X_3}$ is \mathcal{X}_3 -symmetrizable by $\mathcal{X}_1/\mathcal{X}_2$ if, for each $(\tilde{x}_1, x_2, x_3, \tilde{x}_3)$, the conditional output distributions in the two cases above are the same. The receiver is unable to tell whether user-3 is sending x_3 (and user-1 being malicious) or user-3 is sending \tilde{x}_3 (and user-2 being malicious).

$$= \sum_{\tilde{x}_i} q(\tilde{x}_i|x_j, x_k) W_{Y|X_i X_j X_k}(y|\tilde{x}_i, \tilde{x}_j, \tilde{x}_k), \\ \forall x_j, \tilde{x}_j \in \mathcal{X}_j, x_k, \tilde{x}_k \in \mathcal{X}_k, y \in \mathcal{Y}. \quad (6)$$

2) We say that $W_{Y|X_1X_2X_3}$ is $\mathcal{X}_k|\mathcal{X}_j$ -symmetrizable by \mathcal{X}_i if for some distribution $q(x_i|\tilde{x}_k)$

$$\sum_{x_i} q(x_i|\tilde{x}_k) W_{Y|X_i X_j X_k}(y|x_i, x_j, x_k) \\ = \sum_{\tilde{x}_i} q(\tilde{x}_i|x_k) W_{Y|X_i X_j X_k}(y|\tilde{x}_i, x_j, \tilde{x}_k), \\ \forall x_j \in \mathcal{X}_j, x_k, \tilde{x}_k \in \mathcal{X}_k, y \in \mathcal{Y}. \quad (7)$$

3) We say that $W_{Y|X_1X_2X_3}$ is \mathcal{X}_k -symmetrizable by $\mathcal{X}_i/\mathcal{X}_j$ if for some pair of distributions $q(x_i|\tilde{x}_i, \tilde{x}_k)$ and $q'(\tilde{x}_j|x_j, x_k)$

$$\sum_{x_i} q(x_i|\tilde{x}_i, \tilde{x}_k) W_{Y|X_i X_j X_k}(y|x_i, x_j, x_k) \\ = \sum_{\tilde{x}_j} q'(\tilde{x}_j|x_j, x_k) W_{Y|X_i X_j X_k}(y|\tilde{x}_i, \tilde{x}_j, \tilde{x}_k), \\ \forall \tilde{x}_i \in \mathcal{X}_i, x_j \in \mathcal{X}_j, x_k, \tilde{x}_k \in \mathcal{X}_k, y \in \mathcal{Y}. \quad (8)$$

We say that *user-k is symmetrizable* if any of the above three symmetrizable conditions (6)-(8) holds for some distinct $i, j \in \{1, 2, 3\} \setminus \{k\}$. We say that the channel is *not symmetrizable* if user-k is not symmetrizable for every $k \in \{1, 2, 3\}$. In Section V-C, we generalize the symmetrizable conditions to more than three users and provide a unified way of looking at them.

The first two symmetrizable conditions arise from the possibility that the decoder cannot tell apart different messages of honest user(s) when a particular user behaves adversarially. These symmetrizable conditions for the two-user AV-MAC with X_i as the state and X_j, X_k as the inputs are also symmetrizable conditions for our problem. Thus, the first two conditions (6)-(7) (Figures 5 and 6) follow from two-user AV-MAC symmetrizable conditions given by Gubner [9]. Notice that (6) involves a distribution $q(x_i|x_j, x_k)$ whereas (7) involves $q(x_i|x_k)$. The third condition (8) (Figure 7) is new (see Section III-B1e) and arises from the byzantine nature of the users in this problem. In a byzantine-MAC, the decoder may not be able to tell apart two messages since while one message is explained by the possibility of another user (say j) behaving adversarially, the other message may be explained by the possibility of a third user (say k) behaving adversarially. We discuss the implications of the third condition in Section III-B1b where we

argue that a symmetrizable user cannot communicate reliably using deterministic codes.

b) *Symmetrizable implies non-feasibility of communication:* Suppose that (8) holds for $(i, j, k) = (1, 2, 3)$. Thus, user-3 is symmetrizable. In the following, we show that user-3 cannot communicate reliably at positive rates. For fixed vectors $(\tilde{\mathbf{x}}_1, \mathbf{x}_2, \mathbf{x}_3, \tilde{\mathbf{x}}_3)$, Eq. (8) with $(i, j, k) = (1, 2, 3)$ implies that the output is same under the following two cases:

- (i) User 1 sends $\mathbf{X}_1 \sim q^n(\cdot | \tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_3)$, i.e., a vector distributed as the output of the memoryless channel q on input $(\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_3)$ (see Figure 7 which depicts single use of the channel), user-2 and user-3 send \mathbf{x}_2 and \mathbf{x}_3 respectively, and
- (ii) User 2 sends $\mathbf{X}_2 \sim (q')^n(\cdot | \mathbf{x}_2, \mathbf{x}_3)$, and user-1 and user-3 send $\tilde{\mathbf{x}}_1$ and $\tilde{\mathbf{x}}_3$ respectively.

Hence, for a given $(\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, n)$ code (f_1, f_2, f_3, ϕ) and independent $\tilde{M}_1 \sim \text{Unif}(\mathcal{M}_1)$, $M_2 \sim \text{Unif}(\mathcal{M}_2)$, $M_3 \sim \text{Unif}(\mathcal{M}_3)$ and $\tilde{M}_3 \sim \text{Unif}(\mathcal{M}_3)$, the output distributions are identical in the following two cases:

- (i) User 1 sends $\mathbf{X}_1 \sim q^n(\cdot | f_1(\tilde{M}_1), f_3(\tilde{M}_3))$, user-2 and user-3 send $f_2(M_2)$ and $f_3(M_3)$ respectively, and
- (ii) User 2 sends $\mathbf{X}_2 \sim (q')^n(\cdot | f_2(M_2), f_3(M_3))$, and user-1 and user-3 send $f_1(M_1)$ and $f_3(M_3)$ respectively.

Thus, the receiver is unable to tell apart the two possibilities, i.e., whether user-1 is malicious with user-3 sending M_3 or user-2 is malicious with user-3 sending \tilde{M}_3 . We can argue along the similar lines to show that the symmetrized user(s) in (6) or (7) cannot communicate reliably. On the other hand, we can show that when no user is symmetrizable, we can work at positive rates. This brings us to our main result.

c) *Deterministic capacity region:* Let \mathcal{R} be the set of all rate triples (R_1, R_2, R_3) such that for some $p(u)p(x_1|u)p(x_2|u)p(x_3|u)$, the following conditions hold for all permutations (i, j, k) of $(1, 2, 3)$:

$$R_i \leq \min_{q(x_k|u)} I(X_i; Y|X_j, U), \quad \text{and} \quad (9)$$

$$R_i + R_j \leq \min_{q(x_k|u)} I(X_i, X_j; Y|U), \quad (10)$$

where the mutual information terms above are evaluated using the joint distribution $p(u)p(x_i|u)p(x_j|u)q(x_k|u)W_{Y|X_1X_2X_3}(y|x_1, x_2, x_3)$. Here, U is an auxiliary random variable distributed over some alphabet \mathcal{U} with $|\mathcal{U}| \leq 6$. The bound on the cardinality of \mathcal{U} can be shown using the convex cover method [29, Appendix C].

Theorem 1: $\mathcal{R}_{\text{deterministic}} = \mathcal{R}$ if $W_{Y|X_1X_2X_3}$ is not symmetrizable. Furthermore, $\text{int}(\mathcal{R}_{\text{deterministic}}) \neq \emptyset$ only if $W_{Y|X_1X_2X_3}$ is not symmetrizable.

Remark 1: As argued, we prove the converse part of Theorem 1 by showing that if user- k is symmetrizable, then any achievable rate triple (R_1, R_2, R_3) must be such that $R_k = 0$. Our capacity region characterization does not cover the case where some (but not all) users are symmetrizable. In this case, by Theorem 3 (which shows that $\mathcal{R}_{\text{random}} = \mathcal{R}$), \mathcal{R} restricted to rates of non-symmetrizable users is clearly an outer bound on $\mathcal{R}_{\text{deterministic}}$. It is tempting to conjecture that these regions are equal. A similar result for the two-user

AV-MAC was recently studied by Pereg and Steinberg [11] for the case where the users can privately randomize.

d) *Overview of the proof of Theorem 1:* The detailed proof of Theorem 1 is given in Section IV-A. Here, we describe the main ideas behind the achievability. The codebooks used in the achievability are obtained by a random coding argument (see Lemma 4). We will briefly describe the decoder here and also point out its connection to the non-symmetrizable of the channel. A high-level proof-idea is also given in the flowchart in Figure 12 in Section IV-A (on page 17).

Upon receiving the channel output, the decoder works by separately collecting potential candidates for each user's input message and subjecting them to further checks. Finally, we will show that there will be at most one potential candidate for each user (see Lemma 2) which the decoder outputs. In the following, we describe these steps for decoding user-3's message. Similar procedures are also employed for user-1 and user-2's decoding.

Let \mathcal{C}_i , $i = 1, 2, 3$ denote the codebook of user- i . Given a received vector $\mathbf{y} \in \mathcal{Y}^n$, we say that the message $m_3 \in \mathcal{M}_3$ of user-3 is a "candidate" with an "explanation" $(\mathbf{x}_1, \mathbf{x}_2) \in (\mathcal{X}_1^n \times \mathcal{C}_2) \cup (\mathcal{C}_1 \times \mathcal{X}_2^n)$ if the tuple $(\mathbf{x}_1, \mathbf{x}_2, f_3(m_3), \mathbf{y})$ is jointly typical with respect to a joint distribution that corresponds to independent channel inputs and the channel output following the channel conditional distribution given the inputs. The choice of the set of explanations is motivated by the fact that at most one user can be malicious. Note that, in general, a candidate message may have multiple explanations.

- 1) The decoder first forms a list of all candidate messages of user-3 along with their explanations.
- 2) The list of such candidate messages is then pruned by only keeping those messages that "account" for every other candidate message in the sense described below. Suppose that the candidate message m_3 has an explanation of the form $(\mathbf{x}_1, f_2(m_2))$ for some $\mathbf{x}_1 \in \mathcal{X}_1^n$ and $m_2 \in \mathcal{M}_2$. Similar procedures are followed if the explanation for m_3 is of the form $(f_1(m_1), \mathbf{x}_2)$ by interchanging the roles of user-1 and user-2 below. Let m'_3 be another candidate message. We say that m_3 accounts for m'_3 if one of the following three conditions is satisfied.
- a) m'_3 has an explanation $(\mathbf{x}'_1, f_2(m'_2))$ for some $m'_2 \neq m_2$, such that the collection $(\mathbf{x}_1, f_2(m_2), f_2(m'_2), f_3(m_3), f_3(m'_3), \mathbf{y})$ may be interpreted as typical instances drawn from a distribution $P_{X_1X_2X'_2X_3X'_3Y}$ that specifies that $X'_2X'_3$ and X_2X_3Y are (roughly) conditionally independent given X_1 .
- The condition 2a may be interpreted as follows: \mathbf{x}_1 , $f_2(m_2)$, and $f_3(m_3)$ as inputs to the channel are a more plausible explanation of the channel output than the alternative input $(f_2(m'_2), f_3(m'_3))$, which is part of (adversarial) user-1's attack strategy (see Fig 5a and Fig. 8a). It can be shown that for a non-symmetrizable channel, an analogue of Fig. 5b (see Fig. 8b), which (roughly) corresponds to the Markov chain $X_2X_3 - X_1 - X'_2X'_3Y$, cannot simultaneously hold (also see proof of Lemma 2).

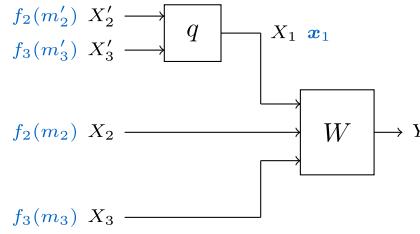
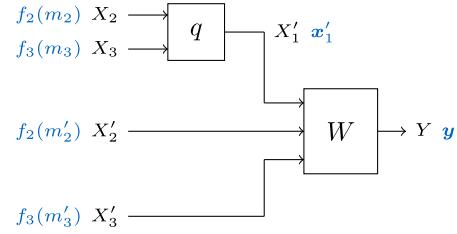
(a) $X'_2 X'_3 - X_1 - X_2 X_3 Y$ Markov chain holds approximately.(b) $X_2 X_3 - X'_1 - X'_2 X'_3 Y$ Markov chain holds approximately.

Fig. 8. The subfigure (a) above describes the decoding condition 2a. The quantities in blue describe it operationally while the random variables describe the single-letter joint distribution. Non-symmetrizability implies that, for $(\mathbf{x}_1, \mathbf{x}'_1, f_2(m_2), f_2(m'_2), f_3(m_3), f_3(m'_3), \mathbf{y}) \in T_{X_1 X'_1 X_2 X'_2 X_3 X'_3 Y}^n$, both (a) and (b) cannot hold simultaneously (see Fig 5).

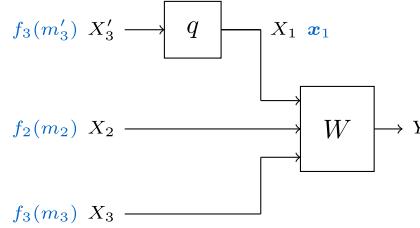
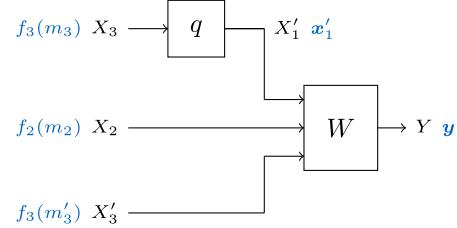
(a) $X'_3 - X_1 - X_2 X_3 Y$ Markov chain holds approximately.(b) $X_3 - X'_1 - X_2 X'_3 Y$ Markov chain holds approximately.

Fig. 9. The subfigure (a) above describes the decoding condition 2b. The quantities in blue describe it operationally while the random variables describe the single-letter joint distribution. Non-symmetrizability implies that, for $(\mathbf{x}_1, \mathbf{x}'_1, f_2(m_2), f_3(m_3), f_3(m'_3), \mathbf{y}) \in T_{X_1 X'_1 X_2 X'_2 X_3 X'_3 Y}^n$, both (a) and (b) cannot hold simultaneously (see Fig 6).

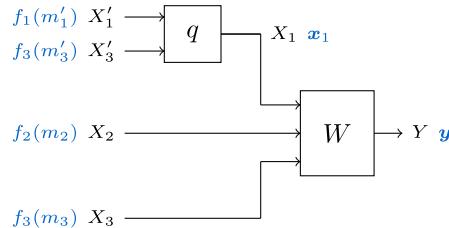
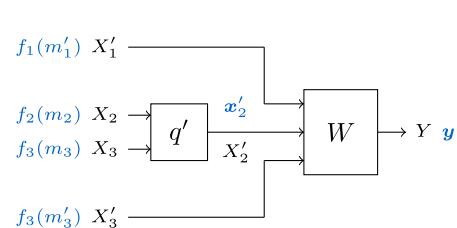
(a) $X'_1 X'_3 - X_1 - X_2 X_3 Y$ Markov chain holds approximately.(b) $X_2 X_3 - X'_2 - X'_1 X'_3 Y$ Markov chain holds approximately.

Fig. 10. The subfigure (a) above describes the decoding condition 2c. The quantities in blue describe it operationally while the random variables describe the single-letter joint distribution. Non-symmetrizability implies that, for $(\mathbf{x}_1, f_1(m'_1), f_2(m_2), \mathbf{x}'_2, f_3(m_3), f_3(m'_3), \mathbf{y}) \in T_{X_1 X'_1 X_2 X'_2 X_3 X'_3 Y}^n$, both (a) and (b) cannot hold simultaneously (see Fig 7).

- b) m'_3 has an explanation $(\mathbf{x}'_1, f_2(m_2))$ such that the collection $(\mathbf{x}_1, f_2(m_2), f_3(m_3), f_3(m'_3), \mathbf{y})$ may be interpreted as typical instances drawn from a distribution $P_{X_1 X_2 X_3 X'_3 Y}$ that specifies that X'_3 and $X_2 X_3 Y$ are (roughly) conditionally independent given X_1 (see Fig. 9).
- c) m'_3 has an explanation $(f_1(m'_1), \mathbf{x}'_2)$ such that the collection $(\mathbf{x}_1, f_1(m'_1), f_2(m_2), f_3(m_3), f_3(m'_3), \mathbf{y})$ may be interpreted as typical instances drawn from a distribution $P_{X_1 X'_1 X_2 X_3 X'_3 Y}$ that specifies that $X'_1 X'_3$ and $X_2 X_3 Y$ are (roughly) conditionally independent given X_1 (see Fig. 10).

See the decoder definition below for a complete description, which accounts for all candidates.

Items (a) and (b) in the decoder definition are similar to the decoding conditions in [10] where user- i is the adversary and \mathbf{x}_i is the state. Item (c) is associated with our new

non-symmetrizability criterion (see Fig. 7) and handles the situation in which an adversarial user tries to make another user appear adversarial while pretending to act honestly.

i) Decoder: Let $\eta > 0$. For a received vector $\mathbf{y} \in \mathcal{Y}^n$, the decoder outputs $\phi(\mathbf{y}) = (m_1, m_2, m_3) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$ if $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$ where $\mathcal{D}_{m_i}^{(i)}$, $i = 1, 2, 3$ is defined as below.

$\mathbf{y} \in \mathcal{D}_{m_3}^{(3)}$ if there exists some permutation (i, j) of $(1, 2)$, $m_j \in \mathcal{M}_j$, $\mathbf{x}_i \in \mathcal{X}_i^n$, and random variables X_i, X_j, X_3 with $(\mathbf{x}_i, f_j(m_j), f_3(m_3), \mathbf{y}) \in T_{X_i X_j X_3 Y}^n$ and $D(P_{X_i X_j X_3 Y} \| P_{X_i} \times P_{X_j} \times P_{X_3} \times W) < \eta$ such that the following hold:

- (a) **Disambiguating (m_j, m_3) from (m'_j, m'_3) :** For every $(m'_j, m'_3) \in \mathcal{M}_j \times \mathcal{M}_3$, $m'_j \neq m_j$, $m'_3 \neq m_3$, $\mathbf{x}'_i \in \mathcal{X}_i^n$, and random variables X'_i, X'_j, X'_3 such that $(\mathbf{x}_i, \mathbf{x}'_i, f_j(m_j), f_3(m_3), f_3(m'_3), \mathbf{y}) \in$

$T_{X_i X'_i X_j X'_j X_3 X'_3 Y}^n$ and $D(P_{X_i' X_j' X_3' Y} || P_{X'_1} \times P_{X'_j} \times P_{X'_3} \times W) < \eta$, we require that $I(X_j X_3 Y; X'_j X'_3 | X_i) < \eta$.

(b) **Disambiguating m_3 from m'_3 :** For every $m'_3 \in \mathcal{M}_3$, $m'_3 \neq m_3$, $x'_i \in \mathcal{X}_i^n$, and random variables X'_i, X'_3 such that $(\mathbf{x}_i, \mathbf{x}'_i, f_j(m_j), f_3(m_3), f_3(m'_3), \mathbf{y}) \in T_{X_i X'_i X_j X'_j X_3 X'_3 Y}^n$ and $D(P_{X_i' X_j' X_3' Y} || P_{X'_1} \times P_{X'_j} \times P_{X'_3} \times W) < \eta$, we require that $I(X_j X_3 Y; X'_3 | X_i) < \eta$.

(c) **Disambiguating (m_j, m_3) from (m_i, m'_3) :** If there exist $(m_i, m'_3) \in \mathcal{M}_i \times \mathcal{M}_3$, $m'_3 \neq m_3$, $x_j \in \mathcal{X}_j^n$, and random variables X'_i, X'_j, X'_3 such that $(\mathbf{x}_i, f_i(m_i), f_j(m_j), \mathbf{x}_j, f_3(m_3), f_3(m'_3), \mathbf{y}) \in T_{X_i X'_i X_j X'_j X_3 X'_3 Y}^n$ and $D(P_{X_i' X_j' X_3' Y} || P_{X'_1} \times P_{X'_j} \times P_{X'_3} \times W) < \eta$, we require that $I(X_j X_3 Y; X'_i X'_3 | X_i) < \eta$.

The decoding sets $\mathcal{D}_{m_1}^{(1)}$ and $\mathcal{D}_{m_2}^{(2)}$ are defined similarly. If $\mathbf{y} \notin \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$ for all $(m_1, m_2, m_3) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$, the decoder outputs $(1, 1, 1)$.

Note that the decoder is not well defined if $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$ and $\mathbf{y} \in \mathcal{D}_{m'_1}^{(1)} \cap \mathcal{D}_{m'_2}^{(2)} \cap \mathcal{D}_{m'_3}^{(3)}$ for $(m_1, m_2, m_3) \neq (m'_1, m'_2, m'_3)$. This is ruled out by the following lemma (proved in Appendix I) which guarantees that, for sufficiently small $\eta > 0$, there is at most one triple (m_1, m_2, m_3) such that $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$. This is analogous to [22, Lemma 4].

Lemma 2 (Disambiguity of Decoding): Suppose the channel $W_{Y|X_1 X_2 X_3}$ is not symmetrizable. Let $P_{X_1} \in \mathcal{P}_{\mathcal{X}_1}^n$, $P_{X_2} \in \mathcal{P}_{\mathcal{X}_2}^n$ and $P_{X_3} \in \mathcal{P}_{\mathcal{X}_3}^n$ be distributions such that for some $\alpha > 0$, $\min_{x_1} P_{X_1}(x_1), \min_{x_2} P_{X_2}(x_2), \min_{x_3} P_{X_3}(x_3) \geq \alpha$. Let $f_1 : \mathcal{M}_1 \rightarrow T_{X_1}^n$, $f_2 : \mathcal{M}_2 \rightarrow T_{X_2}^n$ and $f_3 : \mathcal{M}_3 \rightarrow T_{X_3}^n$ be any encoding maps. There exists a choice of $\eta > 0$ such that if $(\tilde{m}_1, \tilde{m}_2, \tilde{m}_3) \neq (m_1, m_2, m_3)$, then $(\mathcal{D}_{\tilde{m}_1}^{(1)} \cap \mathcal{D}_{\tilde{m}_2}^{(2)} \cap \mathcal{D}_{\tilde{m}_3}^{(3)}) \cap (\mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}) = \emptyset$.

Notice that the decoder definition does not require consistency of the input message for the same user. For example, when $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$, in which case the decoder outputs (m_1, m_2, m_3) , the message m_2 plays no special role in $\mathcal{D}_{m_1}^{(1)}$ or $\mathcal{D}_{m_3}^{(3)}$. That is, an “explanation” for the candidate m_1 may be $(f_2(\tilde{m}_2), \mathbf{x}_3) \in \mathcal{X}_2^n \times \mathcal{X}_3^n$ which passes checks (a), (b) and (c) in the definition of $\mathcal{D}_{m_1}^{(1)}$ where \tilde{m}_2 need not be same as m_2 or even be unique (for instance, there might be another simultaneous “explanation” $(f_2(m'_2), \mathbf{x}'_3)$). At the same time, an “explanation” for the candidate m_3 which passes checks (a), (b) and (c) of $\mathcal{D}_{m_3}^{(3)}$ may be $(\mathbf{x}_1, f_2(\tilde{m}_2)) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$ where \tilde{m}_2 need not be same as \hat{m}_2 or m_2 .

e) “ \mathcal{X}_k -symmetrizable by $\mathcal{X}_i / \mathcal{X}_j$ ” is new: The following example shows that the third symmetrizability condition (8) does not imply the others. The channel below is neither $\mathcal{X}_j \times \mathcal{X}_k$ -symmetrizable by \mathcal{X}_i nor $\mathcal{X}_k | \mathcal{X}_j$ -symmetrizable by \mathcal{X}_i for any permutation (i, j, k) of $(1, 2, 3)$. However, it is \mathcal{X}_3 -symmetrizable by $\mathcal{X}_1 / \mathcal{X}_2$.

Example 1: Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y} = \{0, 1\}^3$ and $\mathcal{X}_3 = \{0, 1\}$. Consider the channel $W_{Y|X_1 X_2 X_3}$ (where the output is $Y = (Y_1, Y_2, Y_3)$) defined by

$$(Y_1, Y_2) = (C_1, C_2),$$

$$Y_3 = \begin{cases} B_1 \oplus (A_1 \odot X_3) & \text{w.p. } 1/2 \\ B_2 \oplus (A_2 \odot X_3) & \text{w.p. } 1/2 \end{cases}$$

where \odot denotes multiplication and \oplus denotes addition modulo 2.

To see that this channel is \mathcal{X}_3 -symmetrizable by $\mathcal{X}_1 / \mathcal{X}_2$, consider the “deterministic” $q((a_1, b_1, c_1) | (\tilde{a}_1, \tilde{b}_1, \tilde{c}_1), \tilde{x}_3)$ and $q'((\tilde{a}_2, \tilde{b}_2, \tilde{c}_2) | (a_2, b_2, c_2), x_3)$, for $(a_1, b_1, c_1), (\tilde{a}_1, \tilde{b}_1, \tilde{c}_1) \in \mathcal{X}_1, (\tilde{a}_2, \tilde{b}_2, \tilde{c}_2), (a_2, b_2, c_2) \in \mathcal{X}_2$ and $\tilde{x}_3, x_3 \in \mathcal{X}_3$, defined as follows: let $g, g' : \{0, 1\}^4 \rightarrow \{0, 1\}^2$ be defined as

$$g((\tilde{a}_1, \tilde{b}_1, \tilde{c}_1), \tilde{x}_3) = (0, \tilde{b}_1 \oplus (\tilde{a}_1 \odot \tilde{x}_3), \tilde{c}_1),$$

$$g'((a_2, b_2, c_2), x_3) = (0, b_2 \oplus (a_2 \odot x_3), c_2).$$

Then

$$q((a_1, b_1, c_1) | (\tilde{a}_1, \tilde{b}_1, \tilde{c}_1), \tilde{x}_3) = 1_{\{(a_1, b_1, c_1) = g((\tilde{a}_1, \tilde{b}_1, \tilde{c}_1), \tilde{x}_3)\}},$$

$$q'((\tilde{a}_2, \tilde{b}_2, \tilde{c}_2) | (a_2, b_2, c_2), x_3) = 1_{\{(\tilde{a}_2, \tilde{b}_2, \tilde{c}_2) = g'((a_2, b_2, c_2), x_3)\}}.$$

Consider the two cases shown in Figure 7 with $\tilde{x}_1 = (\tilde{a}_1, \tilde{b}_1, \tilde{c}_1)$, $x_2 = (a_2, b_2, c_2)$, and q and q' defined as above. It follows that, in both the cases, the channel output Y has the same conditional distribution given each input. In particular,

$$(Y_1, Y_2) = (c_1, c_2),$$

$$Y_3 = \begin{cases} \tilde{b}_1 \oplus (\tilde{a}_1 \odot \tilde{x}_3) & \text{w.p. } 1/2 \\ b_2 \oplus (a_2 \odot x_3) & \text{w.p. } 1/2. \end{cases}$$

This shows that the symmetrizability condition (8) holds for $(i, j, k) = (1, 2, 3)$.

Since $(Y_1, Y_2) = (C_1, C_2)$, it is clear that neither user-1 nor user-2 is symmetrizable. It only remains to be shown that the channel is neither $\mathcal{X}_3 | \mathcal{X}_2$ -symmetrizable by \mathcal{X}_1 nor $\mathcal{X}_3 | \mathcal{X}_1$ -symmetrizable by \mathcal{X}_2 . Suppose the channel is $\mathcal{X}_3 | \mathcal{X}_2$ -symmetrizable by \mathcal{X}_1 . Then, to satisfy (7) for $x_2 = (0, 0, c_2)$ and $(x_3, \tilde{x}_3) = (0, 1)$, it must hold that

$$q(0, 0, 0|1) + q(0, 0, 1|1) + q(1, 0, 0|1) + q(1, 0, 1|1) \\ = q(1, 1, 0|0) + q(1, 1, 1|0) + q(0, 0, 0|0) + q(0, 0, 1|0).$$

However, to satisfy (7) for $x_2 = (1, 0, c_2)$ and $(x_3, \tilde{x}_3) = (0, 1)$, we must also satisfy

$$1 + q(0, 0, 0|1) + q(0, 0, 1|1) + q(1, 0, 0|1) + q(1, 0, 1|1) \\ = q(1, 1, 0|0) + q(1, 1, 1|0) + q(0, 0, 0|0) + q(0, 0, 1|0),$$

which is a contradiction. Hence, the channel is not $\mathcal{X}_3 | \mathcal{X}_2$ -symmetrizable by \mathcal{X}_1 . By symmetry, it is also not $\mathcal{X}_3 | \mathcal{X}_1$ -symmetrizable by \mathcal{X}_2 .

Next, the following examples also show that none of the three types of symmetrizability conditions given in Definition 5 are redundant given the others. Example 2 gives a channel that is $\mathcal{X}_k | \mathcal{X}_j$ -symmetrizable by \mathcal{X}_i for every permutation (i, j, k) of $(1, 2, 3)$ but does not satisfy other any other symmetrizability condition from Definition 5. Example 3 gives a channel that is $\mathcal{X}_1 \times \mathcal{X}_2$ -symmetrizable by \mathcal{X}_3 but does not satisfy other forms of symmetrizability conditions (i.e., conditions of the form 2 and 3 in Definition 5). We skip the detailed proofs here as these properties can be verified following similar arguments as the AVMAC examples from [9] and [10].

Example 2: [9, Example on pg. 264] Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X}_3 = \{0, 1\}$ and $\mathcal{Y} = \{0, 1, 2, 3\}$. Consider the channel $W_{Y|X_1X_2X_3}$ defined by

$$Y = X_1 + X_2 + X_3,$$

where $+$ denotes addition over integers. This channel is $\mathcal{X}_k|\mathcal{X}_j$ -symmetrizable by \mathcal{X}_i but is neither $\mathcal{X}_j \times \mathcal{X}_k$ -symmetrizable by \mathcal{X}_i nor \mathcal{X}_k -symmetrizable by $\mathcal{X}_i/\mathcal{X}_j$ for any permutation (i, j, k) of $(1, 2, 3)$.

Example 3: [10, Example 1] Let $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X}_3 = \mathcal{Y} = \{0, 1\}$. Consider the channel $W_{Y|X_1X_2X_3}$ defined by

$$Y = \begin{cases} X_3 & X_1 \oplus X_2 \oplus X_3 = 0, \\ Z \sim \text{Ber}(1/2) & X_1 \oplus X_2 \oplus X_3 = 1. \end{cases}$$

The channel is $\mathcal{X}_1 \times \mathcal{X}_2$ -symmetrizable by \mathcal{X}_3 but is neither $\mathcal{X}_k|\mathcal{X}_j$ -symmetrizable by \mathcal{X}_i nor \mathcal{X}_k -symmetrizable by $\mathcal{X}_i/\mathcal{X}_j$ for any permutation (i, j, k) of $(1, 2, 3)$.

2) Randomized Coding Capacity Region:

Theorem 3: The randomized coding capacity region of the 3-user byzantine-MAC with at most one adversarial user is given by

$$\mathcal{R}_{\text{random}} = \mathcal{R}_{\text{random}}^{\text{weak}} = \mathcal{R}.$$

Remark 2: The statement $\mathcal{R}_{\text{deterministic}} = \mathcal{R}$, if $\text{int}(\mathcal{R}_{\text{deterministic}}) \neq \emptyset$ can also be shown directly using the extension, provided in [8], of the elimination technique [13] to first show that n^2 -valued randomness at each encoder is sufficient to achieve any rate-triple in $\mathcal{R}_{\text{random}}^{\text{weak}}$ (see Lemma 14). A deterministic code of small rate can be used to send $2 \log_2 n$ bits out of each message. These message bits are then used as the encoder randomness in the next phase to communicate the rest of the message bits using a randomized code.

Below, we sketch the proof of achievability. A detailed achievability proof and a converse proof for the weak adversary case are available in Section IV-B.

Proof Sketch (Achievability of Theorem 3):

The scheme is depicted in Figure 11. The achievability uses the two-user AV-MAC randomized code used in the proof of [8, Theorem 1]. Let (R_1, R_2, R_3) be a rate triple such that, for some $p(u)p(x_1|u)p(x_2|u)p(x_3|u)$, the following conditions hold for all permutations (i, j, k) of $(1, 2, 3)$:

$$\begin{aligned} R_i &< \min_{q(x_k|u)} I(X_i; Y|U, X_j), \quad \text{and} \\ R_i + R_j &< \min_{q(x_k|u)} I(X_i, X_j; Y|U), \end{aligned}$$

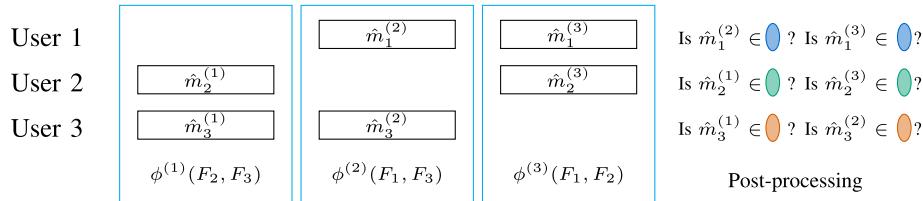
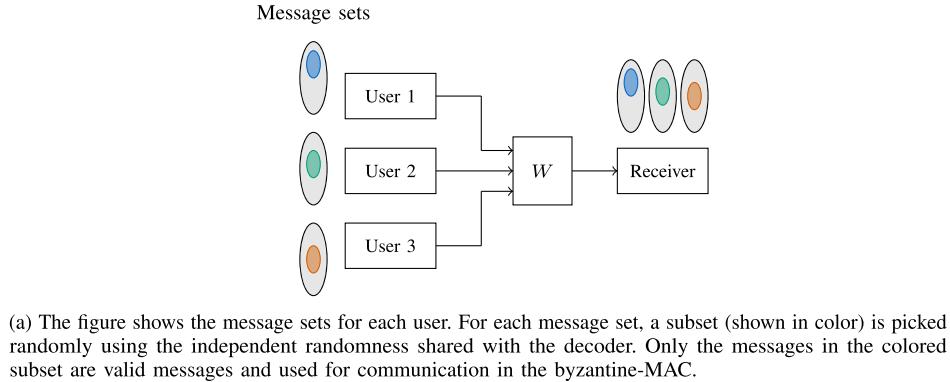
with the mutual information terms evaluated using the joint distribution $p(u)p(x_i|u)p(x_j|u)q(x_k|u)W(y|x_1, x_2, x_3)$. We show the achievability of these rate triplets. Note that for the AV-MAC $W^{(k)}$, the rate pair (R_i, R_j) is achievable by the first part of the direct result of [8, Theorem 1] (see [8, Section III-C]).¹² Here, $W^{(k)}$ is the two-user AV-MAC formed by the channel inputs from user- k as the state and

¹²Note that Jahn's proof does not involve the auxiliary random variable U . However, it can be easily incorporated along the lines of [30].

the remaining channel inputs as the inputs of the legitimate users of the AV-MAC.

In order to design a code for the byzantine-MAC, for each user- $i \in \{1, 2, 3\}$, we consider the randomized encoder F_i which maps each message independently to a codeword generated i.i.d. according to p_i . The realization of each user's codebook is shared with the decoder as independent shared randomness, *i.e.*, F_1, F_2 and F_3 are independent. We note that the encoders F_i and F_j are identical to the ones in the proof of [8, Theorem 1, Section III-C] for the two user AV-MAC $W^{(k)}$. The decoder for the byzantine-MAC will be implemented using the decoders $\phi^{(1)}(F_2, F_3)$, $\phi^{(2)}(F_1, F_3)$ and $\phi^{(3)}(F_1, F_2)$ (from the proof of [8, Theorem 1, Section III-C]) of AV-MACs $W^{(1)}$, $W^{(2)}$ and $W^{(3)}$ corresponding to the encoder pairs (F_2, F_3) , (F_1, F_3) and (F_1, F_2) respectively. It is clear that if, say, user-3 is malicious, and honest users-1 and 2 send m_1 and m_2 respectively, then the output $(\hat{m}_1^{(3)}, \hat{m}_2^{(3)})$ of the decoder $\phi^{(3)}(F_1, F_2)$ will match (m_1, m_2) with high probability. However, since the decoder does not know the identity of the malicious user, there is an additional decoded message $\hat{m}_1^{(2)}$ from decoder $\phi^{(2)}(F_1, F_3)$ for user-1 (and similarly there is an additional decoded message for user-2 from $\phi^{(1)}(F_2, F_3)$). The message $\hat{m}_1^{(2)}$ can potentially be different from $\hat{m}_1^{(3)}$. This is because the decoder $\phi^{(2)}(F_1, F_3)$ assumes that user-3 is honest and no decoding guarantees are available for its output when user-3 is in fact malicious. When $\hat{m}_1^{(3)} \neq \hat{m}_1^{(2)}$, it is not clear what the receiver should output as the decoded message for user-1. This is where we can leverage the independent shared randomness shared by each user with the receiver.

We use a form of random hashing in order to add a further post-processing step which filters the outputs of the decoders of the AV-MACs as follows. Using the randomness they share with the receiver, each user randomly selects a subset of the original message set which is of nearly the same rate but is only a small fraction of original message set in size. These randomly selected subsets will be the valid message sets for communication in the byzantine-MAC. If the decoders of AV-MACs decode to messages which are not in these randomly selected subsets, they will be rejected in the post-processing step. Since these subsets are chosen using the independent shared randomness between each user and the receiver, their identity is hidden from the malicious user. For a malicious user-3, the output of $\phi^{(3)}(F_1, F_2)$ will be correct with high probability and will be accepted in the post-processing step as honest users-1 and 2 will only send valid messages. On the other hand, the outputs of $\phi^{(1)}(F_2, F_3)$ and $\phi^{(2)}(F_1, F_3)$ will be rejected with high probability if they are different from the output of $\phi^{(3)}(F_1, F_2)$. This is because the size of valid message set is only a very small fraction of the original message set, so an arbitrary decoded message will fall outside the set of valid messages with high probability. This crucially uses the fact that these sets are constructed using independent shared randomness which protects the identity of the set of valid messages (and thus the set of valid codewords) and prevents the malicious user from correlating



(b) The decoder works in two steps. Suppose the encoders are F_1 , F_2 and F_3 . To decode user-1's message, the decoder uses the decoder $\phi^{(2)}(F_1, F_3)$ of AV-MAC $W^{(2)}$ and $\phi^{(3)}(F_1, F_2)$ of AV-MAC $W^{(3)}$, to get candidates $\hat{m}_1^{(2)}$ and $\hat{m}_1^{(3)}$ respectively. These candidates pass through a further post-processing step where a candidate which does not belong to the set of valid messages is rejected. If user-1 is honest, at least one of the the decoders among $\phi^{(2)}(F_1, F_3)$ and $\phi^{(3)}(F_1, F_2)$ will output correctly with high probability. Since a small set of valid messages was chosen using independent shared randomness, a malicious user cannot correlate their attack with messages of honest user(s) with high probability. This ensures that erroneous messages are rejected in the post-processing step. The decoder for other users proceeds similarly.

Fig. 11. A figure depicting the decoder for the randomized code of a 3-user byzantine-MAC.

the attack with those messages. These ideas are formalized in Section IV-B. \square

IV. PROOFS

In this section, we present proofs of the results presented in the previous section for the three user byzantine-MAC with at most one adversary.

A. Deterministic Coding Capacity Region (Theorem 1)

Proof (Converse of Theorem 1) The outer bound on the rate region, when non-empty, follows from Theorem 3. Below, we show that a symmetrizable user cannot communicate.

Clearly, symmetrizable conditions for the two-user AV-MAC with \mathcal{X}_i as the state alphabet and $\mathcal{X}_j, \mathcal{X}_k$ as the input alphabets are also symmetrizable conditions for our problem. Conditions 1 and 2 follow from Gubner [9].

To analyze the rate region when condition 3 holds, consider $(i, j, k) = (1, 2, 3)$, the other cases follow similarly. Suppose $q(\tilde{x}_1|x_1, x_3)$ and $q'(\tilde{x}_j|x_j, x_k)$ satisfy (8), i.e.,

$$\begin{aligned} & \sum_{\tilde{x}_1} q(\tilde{x}_1|x_1, \tilde{x}_3) W_{Y|X_1 X_2 X_3}(y|\tilde{x}_1, x_2, x_3) \\ &= \sum_{\tilde{x}_2} q'(\tilde{x}_2|x_2, x_3) W_{Y|X_1 X_2 X_3}(y|x_1, \tilde{x}_2, \tilde{x}_3), \\ & \forall x_1 \in \mathcal{X}_1, x_2 \in \mathcal{X}_2, x_3, \tilde{x}_3 \in \mathcal{X}_3, y \in \mathcal{Y}. \quad (11) \end{aligned}$$

Let $m_3, \tilde{m}_3 \in \mathcal{M}_3$ be distinct, and let $x_3 = f_3(m_3)$ and $\tilde{x}_3 = f_3(\tilde{m}_3)$. We consider two different settings in which user-3 sends x_3 and \tilde{x}_3 respectively:

- (i) In the first setting, user-1 is adversarial. It chooses an $M_1 \sim \text{Unif}(\mathcal{M}_1)$. Let $\mathbf{X}_1 = f_1(M_1)$. To produce its input $\tilde{\mathbf{X}}_{1, \tilde{m}_3}$ to the channel, it passes $(\mathbf{X}_1, \tilde{x}_3)$ through q^n , the n -fold product of the channel $q(\tilde{x}_1|x_1, x_3)$. user-2, being non-adversarial, sends as its input to the channel $\mathbf{X}_2 = f_2(M_2)$, where $M_2 \sim \text{Unif}(\mathcal{M}_2)$. user-3 sends x_3 corresponding to message m_3 . The distribution of the received vector in this case is

$$\begin{aligned} & \frac{1}{N_1 N_2} \sum_{m_1, m_2} \prod_{t=1}^n \sum_{\tilde{x}_{1, \tilde{m}_3, t}} q(\tilde{x}_{1, \tilde{m}_3, t} | f_{1,t}(m_1), \tilde{x}_{3,t}) \\ & \times W_{Y|X_1 X_2 X_3}(y_t | \tilde{x}_{1, \tilde{m}_3, t}, f_{2,t}(m_2), x_{3,t}). \end{aligned}$$

- (ii) In the second setting, user-2 is adversarial. It chooses an $M_2 \sim \text{Unif}(\mathcal{M}_2)$. Let $\mathbf{X}_2 = f_2(M_2)$. To produce its input $\tilde{\mathbf{X}}_{2, m_3}$ to the channel, it passes (\mathbf{X}_2, x_3) through q'^n , the n -fold product of the channel $q'(\tilde{x}_2|x_2, x_3)$. user-1, being non-adversarial now, sends as its input to the channel $\mathbf{X}_1 = f_1(M_1)$, where $M_1 \sim \text{Unif}(\mathcal{M}_1)$. user-3 here sends \tilde{x}_3 corresponding to message \tilde{m}_3 . Here, the distribution of the received vector is

$$\begin{aligned} & \frac{1}{N_1 N_2} \sum_{m_1, m_2} \prod_{t=1}^n \sum_{\tilde{x}_{2, m_3, t}} q'(\tilde{x}_{2, m_3, t} | f_{2,t}(m_2), x_{3,t}) \\ & \times W_{Y|X_1 X_2 X_3}(y_t | f_{1,t}(m_1), \tilde{x}_{2, m_3, t}, \tilde{x}_{3,t}). \end{aligned}$$

By (11), the above two distributions are identical. Hence, for any decoder, the sum of probabilities of decoding error for messages m_3 and \tilde{m}_3 must be at least 1, i.e., if we

define $e_1^3(m_3, \tilde{\mathbf{x}}_1) \stackrel{\text{def}}{=} \frac{1}{N_2} \sum_{m'_2} e_1(\tilde{\mathbf{x}}_1, m'_2, m_3)$ and similarly $e_2^3(\tilde{m}_3, \tilde{\mathbf{x}}_2) \stackrel{\text{def}}{=} \frac{1}{N_1} \sum_{m'_1} e_2(m'_1, \tilde{\mathbf{x}}_2, \tilde{m}_3)$, then

$$\begin{aligned} & \mathbb{E}_{\tilde{\mathbf{X}}_{1,\tilde{m}_3}} [e_1^3(m_3, \tilde{\mathbf{X}}_{1,\tilde{m}_3})] + \mathbb{E}_{\tilde{\mathbf{X}}_{2,m_3}} [e_2^3(\tilde{m}_3, \tilde{\mathbf{X}}_{2,m_3})] \\ &= \sum_{\mathbf{y}: \phi(\mathbf{y}) \neq m_3} \left(\frac{1}{N_1 N_2} \sum_{m_1, m_2} \prod_{t=1}^n \sum_{\tilde{x}_{1,t}} q(\tilde{x}_{1,t} | f_{1,t}(m_1), \tilde{x}_{3,t}) \right. \\ & \quad \left. W_{Y|X_1 X_2 X_3}(y_t | \tilde{x}_{1,t}, f_{2,t}(m_2), x_{3,t}) \right) \\ & \quad + \sum_{\mathbf{y}: \phi(\mathbf{y}) \neq \tilde{m}_3} \left(\frac{1}{N_1 N_2} \sum_{m_1, m_2} \prod_{t=1}^n \sum_{\tilde{x}_{2,t}} q'(\tilde{x}_{2,t} | f_{2,t}(m_2), x_{3,t}) \right. \\ & \quad \left. W_{Y|X_1 X_2 X_3}(y_t | f_{1,t}(m_1), \tilde{x}_{2,t}, \tilde{x}_{3,t}) \right) \\ & \stackrel{(a)}{\geq} 1, \end{aligned}$$

where (a) follows from (11).

Note that the distribution of $\tilde{\mathbf{X}}_1$ (resp. $\tilde{\mathbf{X}}_2$) does not depend on m_3 (resp. \tilde{m}_3). Arguing along the lines of [22, (3.29) in page 187],

$$\begin{aligned} & 2P_e(f_1, f_2, f_3, \phi) \\ & \geq P_{e,1} + P_{e,2} \\ & \geq \frac{1}{N_3} \sum_{m_3} \mathbb{E}_{\tilde{\mathbf{X}}_1} [e_1^3(m_3, \tilde{\mathbf{X}}_1)] + \frac{1}{N_3} \sum_{m_3} \mathbb{E}_{\tilde{\mathbf{X}}_2} [e_1^3(m_3, \tilde{\mathbf{X}}_2)] \end{aligned}$$

for any attack vectors $\tilde{\mathbf{X}}_1$ and $\tilde{\mathbf{X}}_2$. In particular, for the attack vectors $\frac{1}{N_3} \sum_{\tilde{m}_3} \tilde{\mathbf{X}}_{1,\tilde{m}_3}$ and $\frac{1}{N_3} \sum_{m_3} \tilde{\mathbf{X}}_{2,m_3}$,

$$\begin{aligned} & 2P_e(f_1, f_2, f_3, \phi) \\ & \geq \frac{1}{N_3^2} \sum_{\tilde{m}_3} \sum_{m_3} \left(\mathbb{E}_{\tilde{\mathbf{X}}_{1,\tilde{m}_3}} [e_1^3(m_3, \tilde{\mathbf{X}}_{1,\tilde{m}_3})] \right. \\ & \quad \left. + \mathbb{E}_{\tilde{\mathbf{X}}_{2,m_3}} [e_2^3(\tilde{m}_3, \tilde{\mathbf{X}}_{2,m_3})] \right). \end{aligned}$$

For $m_3 \neq \tilde{m}_3$, the term in brackets on the right is upper bounded by 1, otherwise it is upper bounded by zero. Thus,

$$\begin{aligned} P_e(f_1, f_2, f_3, \phi) & \geq \frac{N_3(N_3 - 1)/2}{2N_3^2} \\ & \geq \frac{1}{8}. \end{aligned}$$

□

Next, we turn to achievability of Theorem 1. It uses [24, Theorem 2.1] which provides a concentration result for dependent random variables. We use it to obtain the codebook given below. This codebook is a generalization of the codebook for the point-to-point AVC (Lemma 3) studied in [22]. In particular, (12), shown at the bottom of the next page, is similar to [22, Lemma 3, (3.1)]. (13) and (14), shown at the bottom of the next page, respectively are generalizations of [22, Lemma 3, (3.1)] to a pair of messages. Similarly, (15), shown at the bottom of the next page is a generalization of [22, Lemma 3, (3.2)], and (16), (17) and (18), shown at the bottom of the next page, respectively are generalizations of [22, Lemma 3, (3.3)]. As we mentioned in Section I-D2, proving these generalizations requires establishing an analogue of the concentration result [22, Lemma A1] for multi-user channels.

We specialize the concentration result in [24, Theorem 2.1] to obtain such an extension. We illustrate the proof idea by proving (13) immediately following the lemma statement. For the complete proof, please refer to Appendix II.

Lemma 4 (Codebook Lemma): For any $\epsilon > 0$, $n \geq n_0(\epsilon)$, $N_1, N_2, N_3 \geq \exp(ne)$ and types $P_1 \in \mathcal{P}_{\mathcal{X}_1^n}$, $P_2 \in \mathcal{P}_{\mathcal{X}_2^n}$, $P_3 \in \mathcal{P}_{\mathcal{X}_3^n}$, there exists codebooks $\mathbf{x}_{11}, \dots, \mathbf{x}_{1N_1} \in \mathcal{X}_1^n$, $\mathbf{x}_{21}, \dots, \mathbf{x}_{2N_2} \in \mathcal{X}_2^n$, $\mathbf{x}_{31}, \dots, \mathbf{x}_{3N_3} \in \mathcal{X}_3^n$ whose codewords are of type P_1, P_2, P_3 respectively such that for every permutation (i, j, k) of $(1, 2, 3)$; for every $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$; for every joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}$; and for $R_i \stackrel{\text{def}}{=} (1/n) \log_2 N_i$, $R_j \stackrel{\text{def}}{=} (1/n) \log_2 N_j$, and $R_k \stackrel{\text{def}}{=} (1/n) \log_2 N_k$; the statements (12)–(18), shown at the bottom of the next page.

Proof Idea: The existence of a codebook satisfying properties (12)–(18) is shown by a random coding argument. For fixed $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$ and joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}$, we will show that the probability that each of the statements (12)–(18) does not hold, falls doubly exponentially in n . Since $|\mathcal{X}_i^n|$, $|\mathcal{X}_j^n|$, $|\mathcal{X}_k^n|$ and $|\mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}|$ grow only exponentially in n , a union bound will imply the existence of a codebook satisfying (12)–(18). We first restate [24, Theorem 2.1] for ready reference.

Lemma 5: [24, Theorem 2.1] Suppose that $V_\alpha, \alpha \in \mathcal{J}$, is a finite family of non-negative random variables and that \sim is a symmetric relation on the index set \mathcal{J} such that each V_α is independent of $\{V_\beta : \beta \sim \alpha\}$; in other words, the pairs (α, β) with $\alpha \sim \beta$ define the edge set of a (weak) dependency graph for the variables V_α . Let $U := \sum_\alpha V_\alpha$ and $\mu := \mathbb{E}U = \sum_\alpha \mathbb{E}V_\alpha$. Let further, for $\alpha \in \mathcal{J}$, $\tilde{U}_\alpha := \sum_{\beta \sim \alpha} V_\beta$. If $t \geq \mu > 0$, then for every real $r > 0$,

$$\mathbb{P}(U > \mu + t) \leq e^{-r/3} + \sum_{\alpha \in \mathcal{J}} \mathbb{P}\left(\tilde{U}_\alpha > \frac{t}{2r}\right). \quad (19)$$

We will now show the analysis of (13) using Lemma 5. Let $T_l^n, l \in \{1, 2, 3\}$ denote the type class of P_l . We generate independent random codebooks for each user. The codebook for user $l \in \{1, 2, 3\}$, denoted by $(\mathbf{X}_{l1}, \mathbf{X}_{l2}, \dots, \mathbf{X}_{lN_l})$, consists of independent random vectors each distributed uniformly on T_l^n . Fix $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$ and a joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}$ such that for $l \in \{1, 2, 3\}$, $P_{X_l} = P_{X'_l} = P_l$ and $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X_i X_j X_k}^n$.

In order to apply Lemma 5, let $\mathcal{J} = \{(ir, js) : (r, s) \in [1 : N_i] \times [1 : N_j]\}$. For every $(ir, js) \in \mathcal{J}$, we define binary random variable $V_{(ir, js)}$ as

$$V_{(ir, js)} = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{js}) \in T_{X'_i X'_j | X_i X_j X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise} \end{cases}$$

and

$$\begin{aligned} U &= \sum_{(ir, js) \in \mathcal{J}} V_{(ir, js)} \\ &= \left| \{(r, s) \in [1 : N_i] \times [1 : N_j] : (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j | X_i X_j X_k}^n(\mathbf{x}_k)\} \right|. \end{aligned}$$

Note that $(ir, js) \sim (iu, jv)$ if and only if $(ir, js) \cap (iu, jv) \neq \emptyset$. Thus, for $(ir, js) \in \mathcal{J}$, $\tilde{U}_{(ir, js)} = \sum_{(iu, jv) \in \mathcal{J}: (iu, jv) \cap (ir, js) \neq \emptyset} V_{(iu, jv)}$. Next, we will compute $\mu (= \mathbb{E}[U])$. Note that

$$\begin{aligned} & \mathbb{P}(V_{(ir, js)} = 1) \\ &= \frac{|T_{X'_i X'_j | X_i X_j X_k}^n(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k)|}{|T_{X'_i}^n| |T_{X'_j}^n|} \\ &\leq \frac{\exp\{nH(X'_i X'_j | X_i X_j X_k)\}}{(n+1)^{|\mathcal{X}_i|+|\mathcal{X}_j|} \exp\{n(H(X'_i) + H(X'_j))\}} \\ &= (n+1)^{-(|\mathcal{X}_i|+|\mathcal{X}_j|)} \exp\left\{-n(H(X'_i X'_j) - H(X'_i X'_j | X_i X_j X_k) - H(X'_i X'_j) + H(X'_i) + H(X'_j))\right\} \\ &= (n+1)^{-(|\mathcal{X}_i|+|\mathcal{X}_j|)} \exp\{-n(I(X'_i X'_j; X_i X_j X_k) + I(X'_i; X'_j))\} \\ &\leq \exp\{-n(I(X'_i X'_j; X_i X_j X_k) + I(X'_i; X'_j))\} \\ &= \exp\{-n(I(X'_j; X_i X_j X_k) + I(X'_i; X_i X_j X_k | X'_j) + I(X'_i; X'_j))\} \\ &= \exp\{-n(I(X'_j; X_i X_j X_k) + I(X'_i; X'_j X_i X_k X_k))\} \end{aligned}$$

Thus,

$$\begin{aligned} \mu &= \mathbb{E}[U] \\ &= \sum_{(r,s) \in [1:N_i] \times [1:N_j]} \mathbb{E}[V_{(ir, js)}] \end{aligned}$$

$$|\{u \in [1:N_i] : (\mathbf{x}_{iu}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X_i X_j X_k}^n\}| \leq \exp\left(n(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ + \epsilon/2)\right); \quad (12)$$

$$\begin{aligned} & |\{(u, v) \in [1:N_i] \times [1:N_j] : (\mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp\left(n(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_j - I(X'_j; X_i X_j X_k)|^+ - I(X'_i; X'_j | X_i X_j X_k)|^+ + \epsilon/2)\right); \end{aligned} \quad (13)$$

$$\begin{aligned} & |\{(u, w) \in [1:N_i] \times [1:N_k] : (\mathbf{x}_{iu}, \mathbf{x}_{kw}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp\left(n(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_k - I(X'_k; X_i X_j X_k)|^+ - I(X'_i; X'_k | X_i X_j X_k)|^+ + \epsilon/2)\right); \end{aligned} \quad (14)$$

$$\frac{1}{N_i N_j} |\{(r, s) \in [1:N_i] \times [1:N_j] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X_j X_k}^n\}| < \exp\left(-\frac{n\epsilon}{2}\right), \text{ if } I(X_i; X_k) + I(X_j; X_i X_k) \geq \epsilon; \quad (15)$$

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1:N_i] \times [1:N_j] : \exists (u, v) \in [1:N_i] \times [1:N_j], u \neq r, v \neq s, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X'_i X_j X'_i X'_j X_k}^n\}| \\ & < \exp\left(-\frac{n\epsilon}{2}\right), \end{aligned}$$

$$\text{if } I(X_i; X_j X'_i X'_j X_k) + I(X_j; X'_i X'_j X_k) \geq |R_i - I(X'_i; X_k)|^+ + |R_j - I(X'_j; X_k)|^+ - I(X'_i; X'_j | X_k)|^+ + \epsilon; \quad (16)$$

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1:N_i] \times [1:N_j] : \exists (u, w) \in [1:N_i] \times [1:N_k], u \neq r, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{kw}, \mathbf{x}_k) \in T_{X'_i X_j X'_i X'_k X_k}^n\}| \\ & < \exp\left(-\frac{n\epsilon}{2}\right), \end{aligned}$$

$$\text{if } I(X_i; X_j X'_i X'_k X_k) + I(X_j; X'_i X'_k X_k) \geq |R_i - I(X'_i; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ - I(X'_i; X'_k | X_k)|^+ + \epsilon; \quad (17)$$

$$\frac{1}{N_i N_j} |\{(r, s) \in [1:N_i] \times [1:N_j] : \exists u \in [1:N_i], u \neq r, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X'_i X_j X'_i X_k}^n\}| < \exp\left(-\frac{n\epsilon}{2}\right),$$

$$\text{if } I(X_i; X_j X'_i X_k) + I(X_j; X'_i X_k) \geq |R_i - I(X'_i; X_k)|^+ + \epsilon. \quad (18)$$

$$\begin{aligned} &= \sum_{(r,s) \in [1:N_i] \times [1:N_j]} \mathbb{P}(V_{(ir, js)} = 1) \\ &\leq \exp\left\{n(R_i + R_j - I(X'_i; X'_j X_i X_j X_k) - I(X'_j; X_i X_j X_k))\right\} \\ &\leq \exp\left\{n \left| |R_i - I(X'_i; X_i X_j X_k)|^+ + |R_j - I(X'_j; X_i X_j X_k)|^+ - I(X'_i; X'_j | X_i X_j X_k)|^+ \right.\right. \\ &\quad \left.\left. - I(X'_j; X_i X_j X_k)\right|^+ \right\} \\ &:= E. \end{aligned}$$

Let $\nu = \exp(n\epsilon/2)$. We are interested in $\mathbb{P}(U \geq \nu E)$.

$$\begin{aligned} \mathbb{P}(U \geq \nu E) &= \mathbb{P}(U - \mathbb{E}[U] \geq \nu E - \mathbb{E}[U]) \\ &\leq \mathbb{P}(U - \mathbb{E}[U] \geq \nu E - E) \\ &= \mathbb{P}(U \geq \mathbb{E}[U] + (\nu - 1)E) \\ &= \mathbb{P}(U \geq \mu + (\nu - 1)E) \end{aligned}$$

Let $t = (\nu - 1)E$ and $r = \exp(n\epsilon/8)$. We will use (19) now.

$$\begin{aligned} & \mathbb{P}(U > \mu + (\nu - 1)E) \\ & \leq e^{-\frac{1}{3} \exp(n\epsilon/8)} + \sum_{(ir, js) \in \mathcal{J}} \mathbb{P}\left(\tilde{U}_{(ir, js)} > \frac{(\nu - 1)E}{2 \exp(n\epsilon/8)}\right). \end{aligned} \quad (20)$$

$$\begin{aligned} & \text{We need to analyze } \mathbb{P}\left(\tilde{U}_{(ir, js)} > \frac{(\nu - 1)E}{2 \exp(n\epsilon/8)}\right). \\ & \mathbb{P}\left(\tilde{U}_{(ir, js)} > \frac{(\nu - 1)E}{2 \exp(n\epsilon/8)}\right) \end{aligned}$$

$$\begin{aligned}
&= \mathbb{P} \left(\sum_{(iu,jv) \in \mathcal{J}: (iu,jv) \cap (ir,js) \neq \emptyset} V_{(iu,jv)} > \frac{(\nu-1)E}{2 \exp(n\epsilon/8)} \right) \\
&= \mathbb{P} \left(V_{(ir,js)} + \sum_{v \neq s} V_{(ir,jv)} + \sum_{u \neq r} V_{(iu,js)} > \frac{(\nu-1)E}{2 \exp(n\epsilon/8)} \right) \\
&= \mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} + \sum_{u \neq r} V_{(iu,js)} > \frac{(\nu-1)E}{2 \exp(n\epsilon/8)} - V_{(ir,js)} \right) \\
&\leq \mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} + \sum_{u \neq r} V_{(iu,js)} > \frac{(\nu-1)E}{2 \exp(n\epsilon/8)} - 1 \right) \\
&\leq \mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \frac{1}{2} \left(\frac{(\nu-1)E}{2 \exp(n\epsilon/8)} - 1 \right) \right) \\
&\quad + \mathbb{P} \left(\sum_{u \neq r} V_{(iu,js)} > \frac{1}{2} \left(\frac{(\nu-1)E}{2 \exp(n\epsilon/8)} - 1 \right) \right).
\end{aligned}$$

The last inequality uses a union bound. Note that

$$\begin{aligned}
\frac{1}{2} \left(\frac{(\nu-1)E}{2 \exp(n\epsilon/8)} - 1 \right) &= \frac{1}{2} \left(\frac{(\exp(n\epsilon/2) - 1)E}{2 \exp(n\epsilon/8)} - 1 \right) \\
&\geq \frac{1}{2} \left(\frac{(\exp(n\epsilon/2) - 1)E}{2 \exp(n\epsilon/8)} - E \right) \\
&= \frac{1}{2} \left(\left(\frac{(\exp(n\epsilon/2) - 1)}{2 \exp(n\epsilon/8)} - 1 \right) E \right) \\
&\geq \left(\left(\frac{\exp(3n\epsilon/8)}{\exp(n\epsilon/8)} \right) E \right) \text{ for large } n \\
&= \exp(n\epsilon/4).
\end{aligned}$$

Thus,

$$\begin{aligned}
&\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \frac{1}{2} \left(\frac{(\nu-1)E}{2 \exp(n\epsilon/4)} - 1 \right) \right) \\
&\quad + \mathbb{P} \left(\sum_{u \neq r} V_{(iu,js)} > \frac{1}{2} \left(\frac{(\nu-1)E}{2 \exp(n\epsilon/4)} - 1 \right) \right) \\
&\leq \mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \right) \\
&\quad + \mathbb{P} \left(\sum_{u \neq r} V_{(iu,js)} > \exp(n\epsilon/4)E \right).
\end{aligned}$$

Let us first analyze $\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \right)$.

$$\begin{aligned}
&\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \right) \\
&= \sum_{\mathbf{x}_{js} \in T_{X'_j | X_i X_j X_k}^n(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k)} \mathbb{P}(\mathbf{X}_{js} = \mathbf{x}_{js}) \times \\
&\quad \mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \mid \mathbf{X}_{js} = \mathbf{x}_{js} \right).
\end{aligned}$$

We will apply Lemma 5 on $\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/8)E \mid \mathbf{X}_{js} = \mathbf{x}_{js} \right)$ for $\mathcal{J}' = \{(ir, jv) : v \in [1 : N_j] \setminus \{s\}\}$. For every $(ir, jv) \in \mathcal{J}'$, we define binary random variable $V'_{(ir,jv)}$ as

$$V'_{(ir,jv)} = \begin{cases} 1, & \text{if } (\mathbf{X}_{jv}) \in T_{X'_j | X'_i X_i X_j X_k}^n(\mathbf{x}_{ir}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k), \\ 0, & \text{otherwise} \end{cases}$$

and $U' = \sum_{(ir,jv) \in \mathcal{J}'} V'_{(ir,jv)}$. Note that $(ir, jv) \sim (iu, jv')$ if and only if $v = v'$. Next, we will compute $\mathbb{E}[U']$.

$$\begin{aligned}
\mathbb{E}[U'] &= \mathbb{E} \left[\sum_{(ir,jv) \in \mathcal{J}'} V'_{(ir,jv)} \right] \\
&\leq \sum_{v \neq s} \mathbb{P} \left(V'_{(ir,jv)} = 1 \right) \\
&= \sum_{v \neq s} \mathbb{P} \left(\mathbf{X}_{jv} \in T_{X'_j | X'_i X_i X_j X_k}^n(\mathbf{x}_{ir}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \right) \\
&= \sum_{v \neq s} \frac{|T_{X'_j | X'_i X_i X_j X_k}^n(\mathbf{x}_{ir}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k)|}{|T_{X'_j}^n|} \\
&\leq \exp\{nR_j\} \frac{\exp\{nH(X'_j | X'_i X_i X_j X_k)\}}{(n+1)^{|\mathcal{X}_j|} \exp\{nH(X'_j)\}} \\
&\leq \exp\{n(|R_j - I(X'_j; X'_i X_i X_j X_k)|^+)\} \\
&\leq E.
\end{aligned}$$

Now,

$$\begin{aligned}
&\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \mid \mathbf{X}_{js} = \mathbf{x}_{js} \right) \\
&= \mathbb{P} \left(\sum_{(ir,jv) \in \mathcal{J}'} V'_{(ir,jv)} > \exp(n\epsilon/4)E \right) \\
&= \mathbb{P}(U' > \mathbb{E}(U') + \exp(n\epsilon/4)E - \mathbb{E}(U')) \\
&\stackrel{(a)}{\leq} \mathbb{P}(U' > \mathbb{E}(U') + (\exp(n\epsilon/4) - 1)E) \\
&\stackrel{(b)}{\leq} e^{-\frac{1}{3} \exp(n\epsilon/8)} \\
&\quad + \sum_{(ir,jv) \in \mathcal{J}'} \mathbb{P} \left(V'_{(ir,jv)} > \frac{(\exp(n\epsilon/4) - 1)E}{2 \exp(n\epsilon/8)} \right) \\
&\stackrel{(c)}{\leq} e^{-\frac{1}{3} \exp(n\epsilon/8)} + \sum_{(ir,jv) \in \mathcal{J}'} \mathbb{P} \left(V'_{(ir,jv)} > E \right) \text{ for large } n \\
&\stackrel{(d)}{=} e^{-\frac{1}{3} \exp(n\epsilon/8)}
\end{aligned}$$

where (a) holds because $\mathbb{E}[U'] \leq E$, (b) uses (19) for $r = \exp(n\epsilon/8)$, (c) is true for large n and (d) holds because $V'_{(ir,jv)} \in \{0, 1\}$ while $E \geq 1$. Thus,

$$\mathbb{P} \left(\sum_{v \neq s} V_{(ir,jv)} > \exp(n\epsilon/4)E \right) \leq e^{-\frac{1}{3} \exp(n\epsilon/8)}.$$

Similarly,

$$\mathbb{P} \left(\sum_{u \neq r} V_{(iu,js)} > \exp(n\epsilon/4)E \right) \leq e^{-\frac{1}{3} \exp(n\epsilon/8)}.$$

This implies that

$$\mathbb{P}\left(\tilde{U}_{(ir,js)} > \frac{(\nu-1)E}{2\exp(n\epsilon/8)}\right) \leq 2e^{-\frac{1}{3}\exp(n\epsilon/8)}.$$

Thus, from (20),

$$\begin{aligned} & \mathbb{P}(U > \mu + (\nu-1)E) \\ & \leq e^{-\frac{1}{3}\exp(n\epsilon/8)} + |\mathcal{J}|2e^{-\frac{1}{3}\exp(n\epsilon/8)} \\ & = e^{-\frac{1}{3}\exp(n\epsilon/8)} + |N_i||N_j|2e^{-\frac{1}{3}\exp(n\epsilon/8)}, \end{aligned}$$

which falls doubly exponentially. \square

Proof (Achievability of Theorem 1): For an input distribution $p(x_1)p(x_2)p(x_3)$, we first show the achievability of the set of rate triples (R_1, R_2, R_3) which, for all permutations (i, j, k) of $(1, 2, 3)$, satisfy the following conditions:

$$R_i < \min_{q(x_k)} I(X_i; Y|X_j), \quad \text{and} \quad (21)$$

$$R_i + R_j < \min_{q(x_k)} I(X_i, X_j; Y), \quad (22)$$

where the mutual information terms are evaluated using the joint distribution $p(x_i)p(x_j)q(x_k)W(y|x_1, x_2, x_3)$. Fix distributions $P_1 \in \mathcal{P}_{\mathcal{X}_1}^n$, $P_2 \in \mathcal{P}_{\mathcal{X}_2}^n$ and $P_3 \in \mathcal{P}_{\mathcal{X}_3}^n$ (which approach $p(x_1), p(x_2), p(x_3)$ as $n \rightarrow \infty$). For these distributions, consider the codebook given by Lemma 4 and the decoder as given in Definition 6 for some $\eta > 0$ satisfying the condition in Lemma 2. Choose $\epsilon > 0$ such that $\eta > 6\epsilon$. Below, we repeat the decoder from section III-B1d for the sake of completeness.

Definition 6 (Decoder): For a received vector $\mathbf{y} \in \mathcal{Y}^n$, some $\eta > 0$, $\phi(\mathbf{y}) = (m_1, m_2, m_3) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$, if $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$ where $\mathcal{D}_{m_i}^{(i)}$, $i = 1, 2, 3$ is defined as below.

$\mathbf{y} \in \mathcal{D}_{m_1}^{(1)}$ if there exists some permutation (j, k) of $(2, 3)$, $m_j \in \mathcal{M}_j$, $\mathbf{x}_k \in \mathcal{X}_k^n$, and random variables X_1, X_j, X_k, Y with $(f_1(m_1), f_j(m_j), \mathbf{x}_k, \mathbf{y}) \in T_{X_1 X_j X_k Y}^n$ and $D(P_{X_1 X_j X_k Y} || P_{X_1} \times P_{X_j} \times P_{X_k} \times W) < \eta$ such that the following hold:

- (a) **Disambiguating (m_1, m_j) from (m'_1, m'_j) :** For every $(m'_1, m'_j) \in \mathcal{M}_1 \times \mathcal{M}_j$ $m'_1 \neq m_1$, $m'_j \neq m_j$, $\mathbf{x}'_k \in \mathcal{X}_k^n$, and random variables X'_1, X'_j, X'_k such that $(f_1(m_1), f_1(m'_1), f_j(m_j), f_j(m'_j), \mathbf{x}_k, \mathbf{x}'_k, \mathbf{y}) \in T_{X_1 X'_1 X_j X'_j X_k X'_k Y}^n$ and $D(P_{X'_1 X'_j X'_k Y} || P_{X'_1} \times P_{X'_j} \times P_{X'_k} \times W) < \eta$, we require that $I(X_1 X_j Y; X'_1 X'_j | X_k) < \eta$.
- (b) **Disambiguating m_1 from m'_1 :** For every $m'_1 \in \mathcal{M}_1$, $m'_1 \neq m_1$, $\mathbf{x}'_k \in \mathcal{X}_k^n$, and random variables X'_1, X'_k such that $(f_1(m_1), f_1(m'_1), f_j(m_j), \mathbf{x}_k, \mathbf{x}'_k, \mathbf{y}) \in T_{X_1 X'_1 X_j X_k X'_k Y}^n$ and $D(P_{X'_1 X_j X_k X'_k Y} || P_{X'_1} \times P_{X_j} \times P_{X_k} \times W) < \eta$, we require that $I(X_1 X_j Y; X'_1 | X_k) < \eta$.
- (c) **Disambiguating (m_1, m_j) from (m'_1, m_k) :** If there exist $(m'_1, m_k) \in \mathcal{M}_1 \times \mathcal{M}_k$, $m'_1 \neq m_1$, $x_j \in \mathcal{X}_j^n$, and random variables X'_1, X'_j, X'_k such that $(f_1(m_1), f_1(m'_1), f_j(m_j), \mathbf{x}_j, \mathbf{x}_k, f_k(m_k), \mathbf{y}) \in T_{X_1 X'_1 X_j X'_j X_k X'_k Y}^n$ and $D(P_{X'_1 X'_j X'_k Y} || P_{X'_1} \times P_{X'_j} \times P_{X'_k} \times W) < \eta$, we require that $I(X_1 X_j Y; X'_1 X'_k | X_k) < \eta$.

The decoding sets $\mathcal{D}_{m_2}^{(2)}$ and $\mathcal{D}_{m_3}^{(3)}$ are defined similarly. If $\mathbf{y} \notin \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{m_2}^{(2)} \cap \mathcal{D}_{m_3}^{(3)}$ for any $(m_1, m_2, m_3) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$, the decoder outputs $(1, 1, 1)$.

Next, we give some standard properties of joint types as given in [22] (as *Fact 1*, *Fact 2* and *Fact 3*). As mentioned in [22], these bounds can be found in [28]. For finite alphabets \mathcal{X}, \mathcal{Y} , the type class $\mathcal{P}_{\mathcal{X}}^n$, any channel V from \mathcal{X} to \mathcal{Y} and random variables X and Y on \mathcal{X} and \mathcal{Y} respectively with joint distribution P_{XY} , the following holds:

$$|\mathcal{P}_{\mathcal{X}}^n| \leq (n+1)^{|\mathcal{X}|} \quad (23)$$

$$(n+1)^{-|\mathcal{X}|} \exp(nH(X)) \leq |T_X^n(\mathbf{x})| \leq \exp(nH(X)) \quad \text{if } |T_X^n(\mathbf{x})| \neq 0 \quad (24)$$

$$(n+1)^{-|\mathcal{X}||\mathcal{Y}|} \exp(nH(Y|X)) \leq |T_{Y|X}^n(\mathbf{x})| \leq \exp(nH(Y|X)) \quad \text{if } |T_{Y|X}^n(\mathbf{x})| \neq 0 \quad (25)$$

$$\sum_{\mathbf{y} \in T_{Y|X}^n(\mathbf{x})} V^n(\mathbf{y}|\mathbf{x}) \leq \exp(-nD(P_{XY} || P_X \times V)) \quad (26)$$

We first analyze the case when user 3 is adversarial. The probability of error when user 3 is adversarial (see (1)) is given by

$$P_{e,3} \stackrel{\text{def}}{=} \max_{\mathbf{x}_3} P_{e,3}(\mathbf{x}_3),$$

where $P_{e,3}(\mathbf{x}_3)$ is the average probability of error for users 1 and 2 when a malicious user 3 sends \mathbf{x}_3 as input. That is,

$$\begin{aligned} P_{e,3}(\mathbf{x}_3) &:= \frac{1}{N_1 N_2} \sum_{r \in \mathcal{M}_1, s \in \mathcal{M}_2} \mathbb{P}\left(\{\mathbf{y} : \phi(\mathbf{y}) \neq (r, s, t) \right. \\ &\quad \left. \text{for some } t \in \mathcal{M}_3\} \mid \mathbf{X}_1 = \mathbf{x}_{1r}, \mathbf{X}_2 = \mathbf{x}_{2s}, \mathbf{X}_3 = \mathbf{x}_3\right). \end{aligned} \quad (27)$$

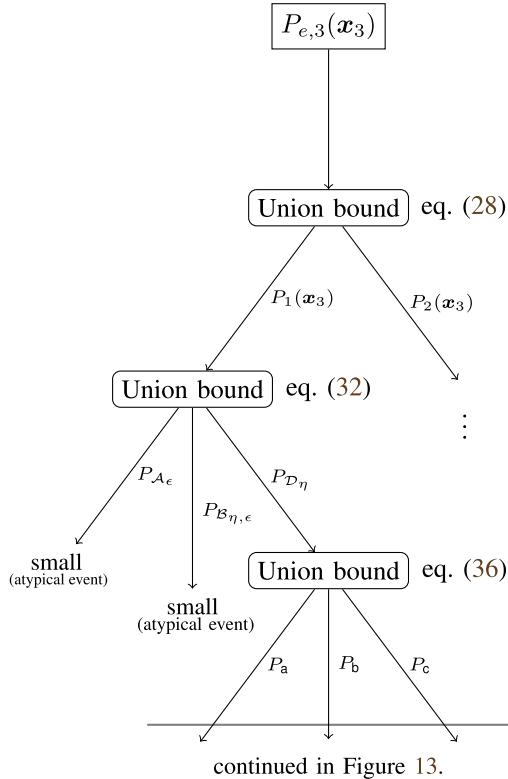
We will argue that for every $\mathbf{x}_3 \in \mathcal{X}_3^n$, $P_{e,3}(\mathbf{x}_3) \rightarrow 0$ as $n \rightarrow \infty$. The analysis of $P_{e,3}(\mathbf{x}_3)$ follows the flowchart shown in Figure 12.

From the decoder definition, we know that for $(r, s) \in \mathcal{M}_1 \times \mathcal{M}_2$, if $\phi(\mathbf{y}) \neq (r, s, t)$ for some $t \in \mathcal{M}_3$, then $\mathbf{y} \notin \mathcal{D}_r^{(1)} \cap \mathcal{D}_s^{(2)}$. In other words, $\mathbf{y} \in (\mathcal{D}_r^{(1)})^c \cup (\mathcal{D}_s^{(2)})^c$. Thus,

$$\begin{aligned} P_{e,3}(\mathbf{x}_3) &= \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n\left(\left\{\mathbf{y} : \mathbf{y} \in (\mathcal{D}_r^{(1)})^c \cup (\mathcal{D}_s^{(2)})^c\right\} \right. \\ &\quad \left. \mid \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3\right) \\ &= \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n\left(\left\{\mathbf{y} : \mathbf{y} \in (\mathcal{D}_r^{(1)})^c\right\} \cup \left\{\mathbf{y} : \mathbf{y} \in (\mathcal{D}_s^{(2)})^c\right\} \right. \\ &\quad \left. \mid \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3\right) \\ &\stackrel{(a)}{\leq} \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n\left(\left\{\mathbf{y} : \mathbf{y} \in (\mathcal{D}_r^{(1)})^c\right\} \mid \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3\right) \\ &\quad + \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n\left(\left\{\mathbf{y} : \mathbf{y} \in (\mathcal{D}_s^{(2)})^c\right\} \mid \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3\right) \end{aligned}$$

where (a) uses the union bound. Thus, for

$$P_1(\mathbf{x}_3) := \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n\left(\left\{\mathbf{y} : \mathbf{y} \notin \mathcal{D}_r^{(1)}\right\} \mid \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3\right),$$



continued in Figure 13.

Fig. 12. Flowchart depicting the flow of analysis of $P_{e,3}(\mathbf{x}_3)$, the average probability of error when malicious user 3 sends \mathbf{x}_3 . In the flowchart, only $P_1(\mathbf{x}_3)$ is further broken down and shown. The flowchart is continued in Figure 13.

and

$$P_2(\mathbf{x}_3) := \frac{1}{N_1 N_2} \sum_{\substack{r \in \mathcal{M}_1 \\ s \in \mathcal{M}_2}} W^n \left(\left\{ \mathbf{y} : \mathbf{y} \notin \mathcal{D}_s^{(2)} \right\} \middle| \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3 \right),$$

we have the following upper bound on $P_{e,3}(\mathbf{x}_3)$.

$$P_{e,3}(\mathbf{x}_3) \leq P_1(\mathbf{x}_3) + P_2(\mathbf{x}_3) \quad (28)$$

We will first analyze $P_1(\mathbf{x}_3)$. Let

$$\mathcal{A}_\epsilon \stackrel{\text{def}}{=} \{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n : D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3}) \geq \epsilon\}, \quad (29)$$

$$\mathcal{B}_{\eta,\epsilon} \stackrel{\text{def}}{=} \{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n : D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3} W) \geq \eta - \epsilon\}, \quad (30)$$

$$\text{and } \mathcal{D}_\eta \stackrel{\text{def}}{=} \{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n : D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3} W) < \eta\}. \quad (31)$$

In defining $\mathcal{B}_{\eta,\epsilon}$, recall that $\eta > 6\epsilon$. We will use \mathcal{A}_ϵ^c , $\mathcal{B}_{\eta,\epsilon}^c$ and \mathcal{D}_η^c to denote $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n \setminus \mathcal{A}_\epsilon$, $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n \setminus \mathcal{B}_{\eta,\epsilon}$ and $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n \setminus \mathcal{D}_\eta$ respectively.

We first note that $\mathcal{A}_\epsilon^c \cap \mathcal{B}_{\eta,\epsilon}^c \subseteq \mathcal{D}_\eta$. This is because $D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3} W) = D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_3} W) + D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3})$ and for $P_{X_1 X_2 X_3} \in \mathcal{A}_\epsilon^c \cap \mathcal{B}_{\eta,\epsilon}^c$, $D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_3} W) + D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3}) < \epsilon + \eta - \epsilon = \eta$. Thus, $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n = \mathcal{A}_\epsilon \cup \mathcal{B}_{\eta,\epsilon} \cup \mathcal{D}_\eta$. We focus on the first term on the RHS of (28) and split the set of joint types $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n$ into \mathcal{A}_ϵ , $\mathcal{B}_{\eta,\epsilon}$ and \mathcal{D}_η . Further, we use loose

$P_{e,3}(\mathbf{x}_3)$	the average probability of error when malicious user 3 sends \mathbf{x}_3
$P_1(\mathbf{x}_3)$	the average probability of error for user 1
$P_2(\mathbf{x}_3)$	the average probability of error for user 2
P_{A_ϵ}	the probability that channel inputs are atypical
$P_{B_{\eta,\epsilon}}$	the probability that the channel output is atypical
$P_{\mathcal{D}_\eta}$	\mathcal{D}_η is such that $\mathcal{A}_\epsilon^c \cap \mathcal{B}_{\eta,\epsilon}^c \subseteq \mathcal{D}_\eta$
P_a	condition (a) in Definition 6 does not hold
P_b	condition (b) in Definition 6 does not hold
P_c	condition (c) in Definition 6 does not hold

upper bounds on each of these terms, for example, in the first terms in (32) below, we upper bound the summand by 1.

$$\begin{aligned}
 P_1(\mathbf{x}_3) &= \frac{1}{N_1 N_2} \sum_{(r,s)} W^n \left(\left\{ \mathbf{y} : \mathbf{y} \notin \mathcal{D}_r^{(1)} \right\} \middle| \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3 \right) \\
 &= \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n} \sum_{(r,s): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
 &\leq \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon} \sum_{(r,s): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n} 1 \\
 &+ \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{B}_{\eta,\epsilon}} \sum_{(r,s): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
 &+ \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta} \sum_{(r,s): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
 &=: P_{A_\epsilon} + P_{B_{\eta,\epsilon}} + P_{\mathcal{D}_\eta}, \tag{32}
 \end{aligned}$$

where we define the $P_{\mathcal{A}_\epsilon}$, $P_{\mathcal{B}_{\eta, \epsilon}}$ and $P_{\mathcal{D}_\eta}$ as the three summation terms. We will analyze each term on the RHS of (32) separately. We start with the first term.

$$\begin{aligned}
P_{\mathcal{A}_\epsilon} &= \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon} \sum_{\substack{(r,s): \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n}} 1 \\
&= \frac{1}{N_1 N_2} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon} |\{(r, s) : (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n\}| \\
&= \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon} \frac{|\{(r, s) : (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n\}|}{N_1 N_2} \\
&\stackrel{(a)}{\leq} \sum_{P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon} \exp(-n\epsilon/2) \\
&\leq |\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n| \exp(-n\epsilon/2) \\
&\stackrel{(b)}{\leq} (n+1)^{|\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}|} \exp(-n\epsilon/2) \\
&\rightarrow 0 \text{ as } n \rightarrow \infty.
\end{aligned}$$

Here, (a) follows from (15) (as $I(X_1; X_3) + I(X_2; X_1 X_3) = D(P_{X_1 X_2 X_3} || P_{X_1} P_{X_2} P_{X_3}) > \epsilon$ for every $P_{X_1 X_2 X_3 Y} \in \mathcal{A}_\epsilon$ as defined in (29)). The inequality (b) uses (23). We now analyze the second term. For fixed $r \in [1 : N_1]$ and $s \in [1 : N_2]$

$$\begin{aligned}
P_{\mathcal{B}_{\eta, \epsilon}} &= \sum_{\substack{P_{X_1 X_2 X_3 Y} \in \mathcal{B}_{\eta, \epsilon}: \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n}} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
&\stackrel{(a)}{\leq} \sum_{\substack{P_{X_1 X_2 X_3 Y} \in \mathcal{B}_{\eta, \epsilon}: \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n}} \exp(-nD(P_{X_1 X_2 X_3 Y} || P_{X_1 X_2 X_3} W)) \\
&\stackrel{(b)}{\leq} \sum_{\substack{P_{X_1 X_2 X_3 Y} \in \mathcal{B}_{\eta, \epsilon}: \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n}} \exp(-n(\eta - \epsilon)) \\
&\leq |\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n| \exp(-n(\eta - \epsilon)) \\
&\stackrel{(c)}{\leq} (n+1)^{|\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}|} \exp(-n(\eta - \epsilon)) \\
&\rightarrow 0 \text{ as } n \rightarrow \infty \text{ as } \eta > 6\epsilon.
\end{aligned}$$

Here, the inequality (a) uses (26), (b) follows by noting that $P_{X_1 X_2 X_3 Y} \in \mathcal{B}_{\eta, \epsilon}$ (see (30)) and thus, $D(P_{X_1 X_2 X_3 Y} || P_{X_1 X_2 X_3} W) > \eta - \epsilon$. The inequality (c) follows because $\mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}}^n \leq (n+1)^{|\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{Y}|}$ by using (23). This shows that the second term on the RHS of (32) also goes to zero as n goes to infinity.

It remains to analyze the third term of (32), that is, $P_{\mathcal{D}_\eta}$. This only involves joint distributions $P_{X_1 X_2 X_3 Y}$ which satisfy $D(P_{X_1 X_2 X_3 Y} || P_{X_1} \times P_{X_2} \times P_{X_3} \times W) \leq \eta$, i.e., $P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta$ (see (31)). When $P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta$, we notice from Definition 6 that $\mathbf{y} \notin \mathcal{D}_r^{(1)}$ only if for each of $(j, k) = (2, 3)$ and $(j, k) = (3, 2)$, at least one of the conditions among (a), (b) and (c) in Definition 6 fails. Thus, to upper bound $P_{\mathcal{D}_\eta}$, it is sufficient to analyze the probability that at least one of

(a)-(c) in Definition 6 fails under $(j, k) = (2, 3)$. This implies that at least one of the following holds:

- (a) There exists $u \in \mathcal{M}_1$, $u \neq r$, $v \in \mathcal{M}_2$, $v \neq s$, $\mathbf{x}'_3 \in \mathcal{X}_3^n$, and random variables X'_1, X'_2, X'_3 such that $(f_1(r), f_2(s), \mathbf{x}_3, f_1(u), f_2(v), \mathbf{x}'_3, \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 X'_2 X'_3 Y}^n$, $D(P_{X'_1 X'_2 X'_3 Y} || P_{X'_1} P_{X'_2} P_{X'_3} W) < \eta$ and $I(X_1 X_2 Y; X'_1 X'_2 | X_3) \geq \eta$.
- (b) There exists $u \in \mathcal{M}_1$, $u \neq r$, $\mathbf{x}'_3 \in \mathcal{X}_3^n$, and random variables X'_1, X'_3 such that $(f_1(r), f_2(s), \mathbf{x}_3, f_1(u), \mathbf{x}'_3, \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 X'_3 Y}^n$, $D(P_{X'_1 X_2 X'_3 Y} || P_{X'_1} P_{X_2} P_{X'_3} W) < \eta$ and $I(X_1 X_2 Y; X'_1 | X_3) \geq \eta$.
- (c) There exists $u \in \mathcal{M}_1$, $u \neq r$, $\mathbf{x}_2 \in \mathcal{X}_2^n$, $w \in \mathcal{M}_3$, and random variables X'_1, X'_2, X'_3 such that $(f_1(r), f_2(s), \mathbf{x}_3, f_1(u), \mathbf{x}_2, f_3(w), \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 X'_2 X'_3 Y}^n$, $D(P_{X'_1 X'_2 X'_3 Y} || P_{X'_1} P_{X'_2} P_{X'_3} W) < \eta$ and $I(X_1 X_2 Y; X'_1 X'_3 | X_3) \geq \eta$.

To analyze these, we define the following sets of distributions:

$$\begin{aligned}
\mathcal{Q}_1 = & \{P_{X_1 X_2 X_3 X'_1 X'_2 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}} : \\
& P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta \cap \mathcal{A}_\epsilon^c, \\
& P_{X'_1 X'_2 X'_3 Y} \in \mathcal{D}_\eta \text{ for some } X'_3, \\
& P_{X_1} = P_{X'_1} = P_1, P_{X_2} = P_{X'_2} = P_2, \text{ and} \\
& I(X_1 X_2 Y; X'_1 X'_2 | X_3) \geq \eta\}
\end{aligned} \tag{33}$$

$$\begin{aligned}
\mathcal{Q}_2 = & \{P_{X_1 X_2 X_3 X'_1 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{X}_1 \times \mathcal{X}_3 \times \mathcal{Y}} : \\
& P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta \cap \mathcal{A}_\epsilon^c, \\
& P_{X'_1 X_2 X'_3 Y} \in \mathcal{D}_\eta \text{ for some } X'_3, \\
& P_{X_1} = P_{X'_1} = P_1, P_{X_2} = P_2, \text{ and} \\
& I(X_1 X_2 Y; X'_1 | X_3) \geq \eta\}
\end{aligned} \tag{34}$$

$$\begin{aligned}
\mathcal{Q}_3 = & \{P_{X_1 X_2 X_3 X'_1 X'_3 Y} \in \mathcal{P}_{\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_3 \times \mathcal{X}_1 \times \mathcal{X}_3 \times \mathcal{Y}} : \\
& P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta \cap \mathcal{A}_\epsilon^c, \\
& P_{X'_1 X'_2 X'_3 Y} \in \mathcal{D}_\eta \text{ for some } X'_2, \\
& P_{X_1} = P_{X'_1} = P_1, P_{X_2} = P_2, P_{X'_3} = P_3, \text{ and} \\
& I(X_1 X_2 Y; X'_1 X'_3 | X_3) \geq \eta\}
\end{aligned} \tag{35}$$

For $r, s \in \mathcal{M}_1 \times \mathcal{M}_2$, $P_{X_1 X_2 X_3 X'_1 X'_2 Y} \in \mathcal{Q}_1$, $P_{X_1 X_2 X_3 X'_1 Y} \in \mathcal{Q}_2$ and $P_{X_1 X_2 X_3 X'_1 X'_3 Y} \in \mathcal{Q}_3$, define the following sets:

$$\begin{aligned}
\mathcal{E}_{r,s,1}(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) &= \{\mathbf{y} : \exists (u, v) \in \mathcal{M}_1 \times \mathcal{M}_2, u \neq r, v \neq s, \\
&\quad (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{2v}, \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 X'_2 Y}^n\} \\
\mathcal{E}_{r,s,2}(P_{X_1 X_2 X_3 X'_1 Y}) &= \{\mathbf{y} : \exists u \in \mathcal{M}_1, u \neq r, \\
&\quad (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 Y}^n\} \\
\mathcal{E}_{r,s,3}(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) &= \{\mathbf{y} : \exists (u, t) \in \mathcal{M}_1 \times \mathcal{M}_3, u \neq r, \\
&\quad (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3t}, \mathbf{y}) \in T_{X_1 X_2 X_3 X'_1 X'_3 Y}^n\}
\end{aligned}$$

Thus,

$$\begin{aligned}
P_{\mathcal{D}_\eta} &= \frac{1}{N_1 N_2} \sum_{r,s} \sum_{\substack{P_{X_1 X_2 X_3 Y} \in \mathcal{D}_\eta: \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \in T_{X_1 X_2 X_3}^n}} 1
\end{aligned}$$

$$\begin{aligned}
& \sum_{\substack{\mathbf{y} \in T_{Y|X_1X_2X_3}^n(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ \mathbf{y} \notin \mathcal{D}_r^{(1)}}} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
& \leq \frac{1}{N_1 N_2} \sum_{r,s} \left\{ \begin{aligned} & \sum_{P_{X_1X_2X_3X'_1X'_2Y} \in \mathcal{Q}_1} W^n(\mathcal{E}_{r,s,1}(P_{X_1X_2X_3X'_1X'_2Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & + \sum_{P_{X_1X_2X_3X'_1Y} \in \mathcal{Q}_2} W^n(\mathcal{E}_{r,s,2}(P_{X_1X_2X_3X'_1Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & + \sum_{P_{X_1X_2X_3X'_1X'_3Y} \in \mathcal{Q}_3} W^n(\mathcal{E}_{r,s,3}(P_{X_1X_2X_3X'_1X'_3Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \end{aligned} \right\} \\
& := P_a + P_b + P_c, \tag{36}
\end{aligned}$$

where

$$\begin{aligned}
P_a &:= \frac{1}{N_1 N_2} \sum_{r,s} \sum_{P_{X_1X_2X_3X'_1X'_2Y} \in \mathcal{Q}_1} W^n(\mathcal{E}_{r,s,1}(P_{X_1X_2X_3X'_1X'_2Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3), \\
& \tag{37}
\end{aligned}$$

$$\begin{aligned}
P_b &:= \frac{1}{N_1 N_2} \sum_{r,s} \sum_{P_{X_1X_2X_3X'_1Y} \in \mathcal{Q}_2} W^n(\mathcal{E}_{r,s,2}(P_{X_1X_2X_3X'_1Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3), \\
& \tag{38}
\end{aligned}$$

$$\begin{aligned}
P_c &:= \frac{1}{N_1 N_2} \sum_{r,s} \sum_{P_{X_1X_2X_3X'_1X'_3Y} \in \mathcal{Q}_3} W^n(\mathcal{E}_{r,s,3}(P_{X_1X_2X_3X'_1X'_3Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3). \\
& \tag{39}
\end{aligned}$$

We have three terms in the summation on the RHS of (36). We will analyze them one after the other. We will start with the first term. The analysis follows the flowchart given in Figure 13.

Analysis of P_a : We will follow the flowchart given in Figure 13. Let

$$\begin{aligned}
& P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y}) \\
& := W^n(\mathcal{E}_{r,s,1}(P_{X_1X_2X_3X'_1X'_2Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3).
\end{aligned}$$

Note that $P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y})$ is upper bounded by the probability of error when r and s are sent by user 1 and user 2 respectively. So, $P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y}) \leq 1$. Thus, from (37), we see that it is sufficient to show that $P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y})$ falls exponentially. Let P_a atypical be the set of joint types satisfying

$$\begin{aligned}
& I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) \\
& \geq \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ \right. \\
& \quad \left. - I(X'_1; X'_2 | X_3) \right|^+ + \epsilon, \tag{40}
\end{aligned}$$

From (16), note that when $P_{X_1X_2X_3X'_1X'_2Y} \in \mathcal{Q}_1$ satisfies (40)

$$\frac{1}{N_1 N_2} \sum_{r,s} P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y}) \tag{41}$$

$$\begin{aligned}
& = \frac{1}{N_1 N_2} \sum_{\substack{(r,s): \exists (u,v) \text{ satisfying} \\ (x_{1r}, x_{2s}, x_3, x_{1u}, x_{2v}) \in T_{X_1X_2X_3X'_1X'_2}^n}} W^n(\{y : y \in \\
& \quad T_{Y|X_1X_2X_3X'_1X'_2}^n(x_{1r}, x_{2s}, x_3, x_{1u}, x_{2v})\} | x_{1r}, x_{2s}, x_3) \\
& \tag{42}
\end{aligned}$$

$$\begin{aligned}
& \leq \frac{1}{N_1 N_2} \left| \{(r,s) \in [1 : N_1] \times [1 : N_2] : \right. \\
& \quad \exists u, v \in [1 : N_1] \times [1 : N_2], u \neq r, v \neq r, \\
& \quad (x_{1r}, x_{2s}, x_{1u}, x_{2v}, x_3) \in T_{X_1X_2X'_1X'_2X_3}^n \} \right| \\
& < \exp\left(-\frac{n\epsilon}{2}\right). \tag{43}
\end{aligned}$$

Otherwise, when

$$\begin{aligned}
& I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) \\
& < \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ \right. \\
& \quad \left. - I(X'_1; X'_2 | X_3) \right|^+ + \epsilon, \tag{44}
\end{aligned}$$

depending on the evaluation of $|R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3)$, we consider four cases:

$$\begin{aligned}
& \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \right|^+ \\
& = 0, \tag{45}
\end{aligned}$$

$$\begin{aligned}
& \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \right|^+ \\
& = R_1 - I(X'_1; X_3) - I(X'_1; X'_2 | X_3), \tag{46}
\end{aligned}$$

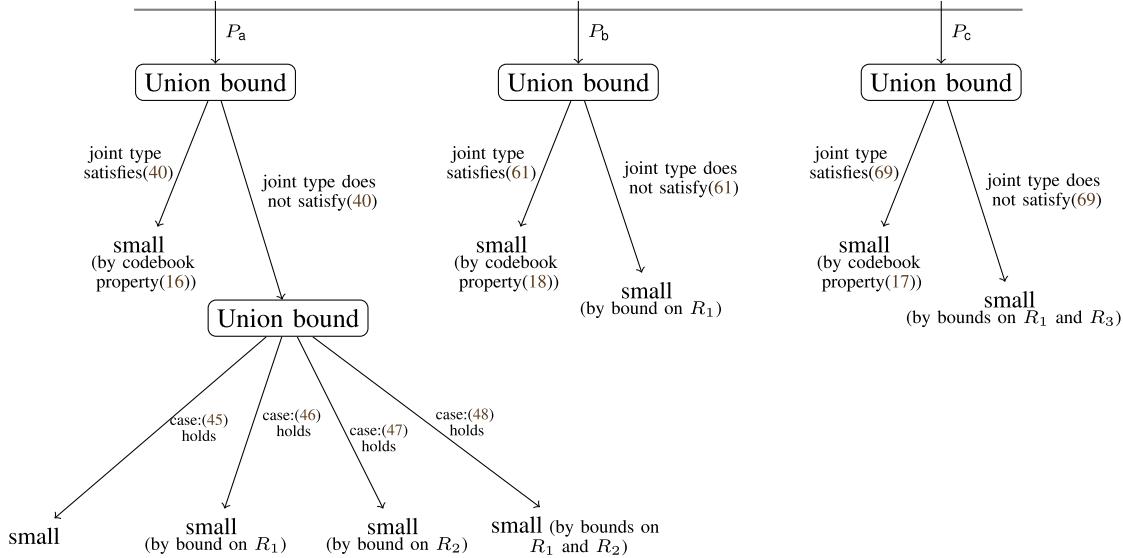
$$\begin{aligned}
& \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \right|^+ \\
& = R_2 - I(X'_2; X_3) - I(X'_1; X'_2 | X_3), \tag{47}
\end{aligned}$$

$$\begin{aligned}
& \left| |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \right|^+ \\
& = R_1 - I(X'_1; X_3) + R_2 - I(X'_2; X_3) - I(X'_1; X'_2 | X_3), \tag{48}
\end{aligned}$$

Before proceeding further, we first argue that (45)-(48) are the only possible evaluations of $|R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3)$. To see this, first suppose $R_1 \leq I(X'_1; X_3)$. If $R_2 \leq I(X'_2; X_3)$, we get (45) as mutual information is always non-negative. When $R_2 > I(X'_2; X_3)$, if $R_2 > I(X'_2; X_3) + I(X'_1; X'_2 | X_3)$, we get (47). Otherwise, we get (45). Next, suppose $R_1 > I(X'_1; X_3)$. In this case, if $R_2 \leq I(X'_2; X_3)$, depending on whether $R_1 > I(X'_1; X_3) + I(X'_1; X'_2 | X_3)$ or not, we get (46) or (45) respectively. When $R_2 > I(X'_2; X_3)$, we get (48) if $R_1 + R_2 > I(X'_1; X_3) + I(X'_2; X_3) + I(X'_1; X'_2 | X_3)$. Otherwise, we get (45).

Analysing each of the cases (45)-(48) separately, we will show that $P_{r,s}^1(P_{X_1X_2X_3X'_1X'_2Y}) \rightarrow 0$ exponentially for each

continued from Figure 12

Fig. 13. Flowchart, continued from Figure 12, depicting the flow of analysis of P_a , P_b and P_c .

$P_{X_1 X_2 X_3 X'_1 X'_2 Y} \in \mathcal{Q}_1$. We will show this by using the following upper bound.

$$\begin{aligned}
 & P_{r,s}^1(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) \\
 &= W^n(\mathcal{E}_{r,s,1}(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
 &\leq \sum_{(u,v):(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{2v}) \in T_{X_1 X_2 X_3 X'_1 X'_2}^n} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\
 &\leq \sum_{(u,v):(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{2v}) \in T_{X_1 X_2 X_3 X'_1 X'_2}^n} \exp(-n(I(Y; X'_1 X'_2 | X_1 X_2 X_3) - \epsilon)) \\
 &\stackrel{(a)}{\leq} \exp\left(n\left(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ - I(X'_1; X'_2 | X_1 X_2 X_3)\right)^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ - I(X'_1; X'_2 | X_1 X_2 X_3) + 3\epsilon/2\right) \quad (49)
 \end{aligned}$$

where (a) follows from (13).

Case 1 (45) Holds: We first note that when

$$\begin{aligned}
 & |R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \\
 &= 0 \quad (50)
 \end{aligned}$$

holds, (44) implies that $I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) < \epsilon$. This further implies the following:

$$\begin{aligned}
 \epsilon &> I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) \\
 &\stackrel{(a)}{\geq} I(X_1; X'_1 X'_2 | X_2 X_3) + I(X_2; X'_1 X'_2 | X_3) \\
 &= I(X_1 X_2; X'_1 X'_2 | X_3) \quad (51)
 \end{aligned}$$

where (a) holds because $I(X_1; X_2 X'_1 X'_2 X_3) = I(X_1; X'_1 X'_2 | X_2 X_3) + I(X_1; X_2 X_3)$ and $I(X_1; X_2 X_3) \geq 0$ as

mutual information is always non-negative. Next, we will argue that when (50) holds, the condition

$$\begin{aligned}
 & |R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ \\
 & - I(X'_1; X'_2 | X_1 X_2 X_3) \geq 0
 \end{aligned}$$

also holds and thus (49) evaluates to $\exp(n(0 - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2))$. We show this by contradiction. Suppose

$$\begin{aligned}
 & |R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ \\
 & - I(X'_1; X'_2 | X_1 X_2 X_3) > 0.
 \end{aligned}$$

This implies that at least one of the conditions out of (i)–(iii) below hold.

$$(i) \quad R_1 > I(X'_1; X_1 X_2 X_3) + I(X'_1; X'_2 | X_1 X_2 X_3), \quad (52)$$

$$(ii) \quad R_2 > I(X'_2; X_1 X_2 X_3) + I(X'_1; X'_2 | X_1 X_2 X_3), \quad (53)$$

$$\begin{aligned}
 (iii) \quad & R_1 > I(X'_1; X_1 X_2 X_3), R_2 > I(X'_2; X_1 X_2 X_3) \text{ and} \\
 & R_1 + R_2 > I(X'_1; X_1 X_2 X_3) + I(X'_2; X_1 X_2 X_3) \\
 & + I(X'_1; X'_2 | X_1 X_2 X_3). \quad (54)
 \end{aligned}$$

If (52) holds, then

$$\begin{aligned}
 R_1 &> I(X'_1; X_1 X_2 X_3) + I(X'_1; X'_2 | X_1 X_2 X_3) \\
 &= I(X'_1; X'_2 X_1 X_2 X_3) \\
 &= I(X'_1; X_3) + I(X'_1; X'_2 | X_3) + I(X'_1; X_1 X_2 | X'_2 X_3) \\
 &\stackrel{(a)}{\geq} I(X'_1; X_3) + I(X'_1; X'_2 | X_3)
 \end{aligned}$$

where (a) follows from non-negativity of mutual information. Note that the inequality (a) contradicts (50). The condition (53) is symmetric and hence leads to a contradiction again. If (54) holds, then $R_1 > I(X'_1; X_1 X_2 X_3) \geq I(X'_1; X_3)$ and $R_2 > I(X'_2; X_1 X_2 X_3) \geq I(X'_2; X_3)$. Furthermore, we have

$$\begin{aligned}
 R_1 + R_2 &= I(X'_1; X_1 X_2 X_3) + I(X'_2; X_1 X_2 X_3) + I(X'_1; X'_2 | X_1 X_2 X_3)
 \end{aligned}$$

$$\begin{aligned}
&= I(X'_1; X'_2 X_1 X_2 X_3) + I(X'_2; X_1 X_2 X_3) \\
&\geq I(X'_1; X_3) + I(X'_1; X'_2 | X_3) + I(X'_2; X_1 X_2 X_3) \\
&\geq I(X'_1; X_3) + I(X'_1; X'_2 | X_3) + I(X'_2; X_3).
\end{aligned}$$

These conditions together contradict (50). Thus,

$$\begin{aligned}
&P_{r,s}^1(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) \\
&\leq \exp(n(-I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2)) \\
&\leq \exp(n(I(X_1 X_2; X'_1 X'_2 | X_3) - I(X_1 X_2 Y; X'_1 X'_2 | X_3) \\
&\quad + 3\epsilon/2)) \\
&\stackrel{(a)}{\leq} \exp(n(\epsilon - \eta + 3\epsilon/2)) \\
&= \exp(n(5\epsilon/2 - \eta)) \\
&\rightarrow 0 \text{ as } \eta > 6\epsilon.
\end{aligned}$$

where (a) uses the fact that $I(X_1 X_2; X'_1 X'_2 | X_3) < \epsilon$ (see (51)) and $I(X_1 X_2 Y; X'_1 X'_2 | X_3) \geq \eta$ (follows from the definition of \mathcal{Q}_1 . See (33)).

Case 2 (46) Holds: We consider the case when

$$\begin{aligned}
&|R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \\
&= R_1 - I(X'_1; X'_2 X_3).
\end{aligned}$$

In this case (44) evaluates to $I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) < R_1 - I(X'_1; X'_2 X_3) + \epsilon$. This implies the following:

$$\begin{aligned}
&\epsilon \\
&> I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) \\
&\quad + I(X'_1; X'_2 X_3) - R_1 \\
&\geq I(X_1; X'_1 | X'_2 X_2 X_3) + I(X_2; X'_1 | X'_2 X_3) \\
&\quad + I(X'_1; X'_2 X_3) - R_1 \\
&= I(X'_1; X_1 X_2 X_3 X'_2) - R_1.
\end{aligned}$$

Thus,

$$R_1 - I(X'_1; X_1 X_2 X_3 X'_2) \geq -\epsilon.$$

This implies that

$$|R_1 - I(X'_1; X_1 X_2 X_3)|^+ \leq R_1 - I(X'_1; X_1 X_2 X_3) + \epsilon$$

and we get the following upper bound on (49):

$$\begin{aligned}
&\exp\left(n\left(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ - I(X'_1; X'_2 | X_1 X_2 X_3) + I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2\right)\right) \\
&\leq \exp\left(n(R_1 - I(X'_1; X_1 X_2 X_3 X'_2) + \epsilon + 0 - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2)\right) \\
&\leq \exp\left(n(R_1 - I(X'_1; X_1 X_2 X_3 X'_2 Y) + 5\epsilon/2)\right) \\
&\leq \exp\left(n(R_1 - I(X'_1; X'_2 Y) + 5\epsilon/2)\right) \\
&\leq \exp\left(n\left(R_1 - I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) + \gamma + 5\epsilon/2\right)\right),
\end{aligned} \tag{55}$$

where $P_{\tilde{X}_1 \tilde{X}_2 \tilde{X}_3 \tilde{Y}} \stackrel{\text{def}}{=} P_{X'_1} \times P_{X'_2} \times P_{X'_3} \times W$ and γ is chosen to satisfy $I(X'_1; X'_2 Y) \geq I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) - \gamma$. Note that $P_{X'_1 X'_2 X'_3 Y}$ is such that $D(P_{X'_1 X'_2 X'_3 Y} || P_{X'_1} \times P_{X'_2} \times P_{X'_3} \times W) < \eta$ where η can be chosen arbitrarily small. Thus, $P_{X'_1 X'_2 X'_3 Y}$ is

arbitrarily close to $P_{\tilde{X}_1 \tilde{X}_2 \tilde{X}_3 \tilde{Y}}$ and γ can be chosen arbitrarily small. Thus, $P_{r,s}^1(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) \rightarrow 0$ exponentially, if

$$R_1 < I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) - \gamma - 5\epsilon/2.$$

Minimizing this in the limit of $n \rightarrow \infty$ and $\epsilon, \eta \rightarrow 0$ over all $P_{X_1 X_2 X_3 X'_1 X'_2 Y} \in \mathcal{Q}_1$ is same as minimizing $I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2)$ over $P_{\tilde{X}_1 \tilde{X}_2 \tilde{X}_3 \tilde{Y}} \in \mathcal{P}_3$ where \mathcal{P}_3 is defined as

$$\mathcal{P}_3 \stackrel{\text{def}}{=} \{P_{X_1 X_2 X_3 Y} : P_{X_1 X_2 X_3 Y} = P_{X_1} \times P_{X_2} \times P_{X_3} \times W \text{ for some } Q_{X_3}\}.$$

Using definition of \mathcal{P}_3 , we obtain the following bound on R_1

$$R_1 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_3} I(X_1; Y | X_2). \tag{56}$$

Case 3 (47) Holds: Suppose

$$\begin{aligned}
&|R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \\
&= R_2 - I(X'_2; X'_1 X_3).
\end{aligned}$$

In this case (44) evaluates to $I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) < R_2 - I(X'_2; X'_1 X_3) + \epsilon$. Thus,

$$\begin{aligned}
&\epsilon > I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) + I(X'_2; X'_1 X_3) \\
&\quad - R_2 \\
&\geq I(X_1; X'_2 | X'_1 X_2 X_3) + I(X_2; X'_2 | X'_1 X_3) + I(X'_2; X'_1 X_3) \\
&\quad - R_2 \\
&= I(X'_2; X_1 X_2 X_3 X'_1) - R_2.
\end{aligned}$$

This implies that

$$R_2 - I(X'_2; X_1 X_2 X_3 X'_1) \geq -\epsilon.$$

Thus,

$$|R_2 - I(X'_2; X_1 X_2 X_3 X'_1)|^+ \leq R_2 - I(X'_2; X_1 X_2 X_3 X'_1) + \epsilon.$$

Substituting this in (49), we get the following upper bound:

$$\begin{aligned}
&\exp\left(n(0 + R_2 - I(X'_2; X_1 X_2 X_3 X'_1) + \epsilon - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2)\right).
\end{aligned}$$

This is same as the upper bound in (55) with X'_1 and X'_2 interchanged, and R_1 replaced by R_2 . Thus, we can do a symmetric analysis as in the previous case to obtain the following bound on R_2 :

$$R_2 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_3} I(X_2; Y | X_1) \tag{57}$$

Case 4 (48) Holds: Suppose

$$\begin{aligned}
&|R_1 - I(X'_1; X_3)|^+ + |R_2 - I(X'_2; X_3)|^+ - I(X'_1; X'_2 | X_3) \\
&= R_1 - I(X'_1; X_3) + R_2 - I(X'_2; X'_1 X_3).
\end{aligned}$$

In this case, (44) evaluates to $I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) < R_1 + R_2 - I(X'_1; X_3) + I(X'_2; X'_1 X_3) + \epsilon$. Thus,

$$\begin{aligned}
&\epsilon > I(X_1; X_2 X'_1 X'_2 X_3) + I(X_2; X'_1 X'_2 X_3) + I(X'_1; X_3) \\
&\quad + I(X'_2; X'_1 X_3) - R_1 - R_2 \\
&\geq I(X_1; X'_1 | X'_2 X_3) + I(X_1; X'_2 | X'_1 X_3) + I(X_2; X'_1 | X_3) \\
&\quad + I(X_2; X'_2 | X'_1 X_3) + I(X'_1; X_3) + I(X'_2; X'_1 X_3)
\end{aligned}$$

$$\begin{aligned} & -R_1 - R_2 \\ & = I(X'_1; X_1 X_2 X_3) + I(X'_2; X_1 X_2 X_3 X'_1) - R_1 - R_2. \end{aligned}$$

This implies that

$$\begin{aligned} R_1 - I(X'_1; X_1 X_2 X_3) + R_2 - I(X'_2; X_1 X_2 X_3) \\ - I(X'_1; X'_2 | X_1 X_2 X_3) \geq -\epsilon. \end{aligned}$$

Note that

$$\begin{aligned} & |R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ \\ & - I(X'_1; X'_2 | X_1 X_2 X_3)|^+ \\ & \geq R_1 - I(X'_1; X_1 X_2 X_3) + R_2 - I(X'_2; X_1 X_2 X_3) \\ & - I(X'_1; X'_2 | X_1 X_2 X_3) \\ & \geq -\epsilon. \end{aligned}$$

So,

$$\begin{aligned} & |R_1 - I(X'_1; X_1 X_2 X_3)|^+ + |R_2 - I(X'_2; X_1 X_2 X_3)|^+ \\ & - I(X'_1; X'_2 | X_1 X_2 X_3)|^+ \\ & \leq R_1 - I(X'_1; X_1 X_2 X_3) + R_2 - I(X'_2; X_1 X_2 X_3) \\ & - I(X'_1; X'_2 | X_1 X_2 X_3) + \epsilon. \end{aligned}$$

Thus,

$$\begin{aligned} & P_{r,s}^1(P_{X_1 X_2 X_3 X'_1 X'_2 Y}) \\ & \leq \exp(n(R_1 - I(X'_1; X_1 X_2 X_3) + R_2 - I(X'_2; X_1 X_2 X_3 X'_1) \\ & + \epsilon - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 3\epsilon/2)) \quad (58) \\ & = \exp(n(R_1 - I(X'_1; X_1 X_2 X_3) + R_2 - I(X'_2; X_1 X_2 X_3 X'_1) \\ & - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 5\epsilon/2)) \\ & \leq \exp(n(R_1 + R_2 - I(X'_1 X'_2; X_1 X_2 X_3) \\ & - I(Y; X'_1 X'_2 | X_1 X_2 X_3) + 5\epsilon/2)) \\ & \leq \exp(n(R_1 + R_2 - I(X'_1 X'_2; X_1 X_2 X_3 Y) + 5\epsilon/2)) \\ & \leq \exp(n(R_1 + R_2 - I(X'_1 X'_2; Y) + 5\epsilon/2)). \end{aligned}$$

Following similar steps as earlier, we obtain the following sum rate bound

$$R_1 + R_2 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_3} I(X_1 X_2; Y). \quad (59)$$

Analysis of P_b : Now, we will look at the second term in (36), which is (see (38)),

$$\begin{aligned} P_b := & \sum_{P_{X_1 X_2 X_3 X'_1 Y} \in \mathcal{Q}_2} \frac{1}{N_1 N_2} \\ & \sum_{r,s} W^n(\mathcal{E}_{r,s,2}(P_{X_1 X_2 X_3 X'_1 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3). \quad (60) \end{aligned}$$

Let

$$P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y}) = W^n(\mathcal{E}_{r,s,2}(P_{X_1 X_2 X_3 X'_1 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3).$$

From (18), we see that when $P_{X_1 X_2 X_3 X'_1 Y}$ satisfies

$$I(X_i; X_j X'_i X_k) + I(X_j; X'_i X_k) \geq |R_i - I(X'_i; X_k)|^+ + \epsilon, \quad (61)$$

$$\frac{1}{N_1 N_2} \sum_{r,s} P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y})$$

$$\begin{aligned} & = \frac{1}{N_1 N_2} \sum_{\substack{(r,s): \exists u \text{ satisfying} \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}) \in T_{X_1 X_2 X_3 X'_1}^n}} \\ & \quad \sum_{\mathbf{y} \in T_{Y|X_1 X_2 X_3 X'_1}^n(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u})} \\ & \quad W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \end{aligned} \quad (62)$$

$$\begin{aligned} & \leq \frac{1}{N_1 N_2} |\{(r,s) \in [1:N_1] \times [1:N_2] : \\ & \quad \exists u \in [1:N_1] u \neq r, (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}) \in T_{X_1 X_2 X_3 X'_1}^n\}| \\ & < \exp\left(-\frac{n\epsilon}{2}\right). \end{aligned} \quad (63)$$

Otherwise, when

$$I(X_i; X_j X'_i X_k) + I(X_j; X'_i X_k) < |R_i - I(X'_i; X_k)|^+ + \epsilon, \quad (64)$$

we will show that $P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y})$ falls doubly exponentially for each $P_{X_1 X_2 X_3 X'_1 Y} \in \mathcal{Q}_2$. We will show this by using the following upper bound.

$$\begin{aligned} & P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y}) \quad (65) \\ & = W^n(\mathcal{E}_{r,s,2}(P_{X_1 X_2 X_3 X'_1 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & \leq \sum_{\substack{u: (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}) \\ \in T_{X_1 X_2 X_3 X'_1}^n}} \sum_{\mathbf{y} \in T_{Y|X_1 X_2 X_3 X'_1}^n(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u})} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & \leq \sum_{\substack{u: (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}) \\ \in T_{X_1 X_2 X_3 X'_1}^n}} \exp(-n(I(Y; X'_1 | X_1 X_2 X_3) - \epsilon)) \\ & \stackrel{(a)}{=} \exp\left(n(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ - I(Y; X'_1 | X_1 X_2 X_3) + 3\epsilon/2)\right) \quad (66) \end{aligned}$$

where (a) follows from (12).

Suppose $R_1 \leq I(X'_1; X_2)$, then (64) evaluates to $I(X_1; X_2 X'_1 X_3) + I(X_2; X'_1 X_3) < \epsilon$. Thus, $I(X_1 X_2; X'_1 | X_3) < \epsilon$. We analyze (66) for this case.

$$\begin{aligned} & P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y}) \\ & \leq \exp\left(n(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ - I(Y; X'_1 | X_1 X_2 X_3) + 3\epsilon/2)\right) \\ & = \exp(n(0 - I(Y; X'_1 | X_1 X_2 X_3) + 3\epsilon/2)) \\ & = \exp\left(n(I(X_1 X_2; X'_1 | X_3) - I(X_1 X_2; X'_1 | X_3) \right. \\ & \quad \left. - I(Y; X'_1 | X_1 X_2 X_3) + 3\epsilon/2)\right) \\ & = \exp(n(I(X_1 X_2; X'_1 | X_3) - I(X_1 X_2 Y; X'_1 | X_3) + 3\epsilon/2)) \\ & \stackrel{(a)}{\leq} \exp(n(\epsilon - \eta + 3\epsilon/2)) \\ & \rightarrow 0 \text{ as } \eta > 6\epsilon. \end{aligned}$$

where (a) follows by using $I(X_1 X_2; X'_1 | X_3) < \epsilon$ and $I(X_1 X_2 Y; X'_1 | X_3) \geq \eta$ (see the definition of \mathcal{Q}_2).

Now, we consider the case when $R_1 > I(X'_1; X_2)$. In this case, (64) evaluates to

$$I(X_1; X_2 X'_1 X_3) + I(X_2; X'_1 X_3) < R_1 - I(X'_1; X_3) + \epsilon$$

This implies that $- \epsilon < R_1 - I(X'_1; X_1 X_2 X_3) \leq |R_1 - I(X'_1; X_1 X_2 X_3)|^+$. Thus,

$$\begin{aligned} & |R_1 - I(X'_1; X_1 X_2 X_3)|^+ - I(Y; X'_1 | X_1 X_2 X_3) \\ & \leq R_1 - I(X'_1; X_1 X_2 X_3) - I(Y; X'_1 | X_1 X_2 X_3) + \epsilon \end{aligned}$$

Plugging it into the upper bound on $P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y})$, we obtain

$$\begin{aligned} & P_{r,s}^2(P_{X_1 X_2 X_3 X'_1 Y}) \\ & \leq \exp(n(R_1 - I(X'_1; X_1 X_2 X_3) - I(Y; X'_1 | X_1 X_2 X_3) + 5\epsilon/2)) \\ & = \exp(n(R_1 - I(X'_1; X_1 X_2 X_3 Y) + 5\epsilon/2)) \\ & = \exp(n(R_1 - I(X'_1; X_2 Y) + 5\epsilon/2)) \end{aligned}$$

Since $P_{X'_1 X_2 X'_3 Y}$ is such that $D(P_{X'_1 X_2 X'_3 Y} || P_{X'_1} \times P_{X_2} \times P_{X'_3} \times W) < \eta$ where η can be chosen arbitrarily small, $P_{X'_1 X_2 X'_3 Y}$ is arbitrarily close to $P_{\tilde{X}_1 \tilde{X}_2 \tilde{X}_3 \tilde{Y}} \stackrel{\text{def}}{=} P_{X'_1} \times P_{X_2} \times P_{X'_3} \times W$. So, for small positive number γ_2 , $I(X'_1; X_2 Y) \geq I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) - \gamma_2 \geq \min_{P_{X'_3}} I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) - \gamma_2$. Thus, if

$$R_1 < \min_{P_{\tilde{X}_3}} I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) - 5\epsilon/2 - \gamma_2,$$

$$\text{then, } R_1 \leq \min_{P_{X'_3}} I(X'_1; Y | X_2) - 5\epsilon/2,$$

and therefore, $P_{e_{X_1, X'_1, X_2, X_3 Y}} \rightarrow 0$ as $n \rightarrow 0$. In the limit of $\epsilon \rightarrow 0$, we get

$$R_1 \leq \min_{\substack{P_{X'_3}: P_{\tilde{X}_1 \tilde{X}_2 \tilde{X}_3 \tilde{Y}} \\ = P_{X'_1} \times P_{X_2} \times P_{X'_3} \times W}} I(\tilde{X}_1; \tilde{Y} | \tilde{X}_2) \quad (67)$$

This is same as the upper bound on R_1 given in (56).

Analysis of P_C : We are left with the analysis of the third term in (36), which is given by (see (39))

$$\begin{aligned} P_C &:= \sum_{P_{X_1 X_2 X_3 X'_1 X'_3 Y} \in \mathcal{Q}_3} \frac{1}{N_1 N_2} \sum_{r,s} \\ & W^n(\mathcal{E}_{r,s,3}(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3). \end{aligned} \quad (68)$$

Let

$$\begin{aligned} & P_{r,s}^3(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) \\ & := W^n(\mathcal{E}_{r,s,3}(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3). \end{aligned}$$

When $P_{X_1 X_2 X_3 X'_1 X'_3 Y}$ satisfies the condition (see (17)),

$$\begin{aligned} & I(X_i; X_j X'_i X'_k X_k) + I(X_j; X'_i X'_k X_k) \\ & \geq \left| |R_i - I(X'_i; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ \right. \\ & \quad \left. - I(X'_i; X'_k | X_k) \right|^+ + \epsilon, \end{aligned} \quad (69)$$

$$\frac{1}{N_1 N_2} \sum_{r,s} P_{r,s}^3(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) \quad (70)$$

$$= \frac{1}{N_1 N_2} \sum_{\substack{(r,s): \exists (u,w) \text{ satisfying} \\ (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w}) \in T_{X_1 X_2 X_3 X'_1 X'_3}^n}} \quad$$

$$\sum_{\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w} \in T_{X_1 X_2 X_3 X'_1 X'_3}^n} W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \quad (71)$$

$$\begin{aligned} & \leq \frac{1}{N_1 N_2} \left| \left\{ (r, s) \in [1 : N_1] \times [1 : N_2] : \right. \right. \\ & \quad \exists u, w \in [1 : N_1] \times [1 : N_3], u \neq r, \\ & \quad (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w}) \in T_{X_1 X_2 X_3 X'_1 X'_3}^n \left. \right\} \right| \\ & < \exp\left(-\frac{n\epsilon}{2}\right). \end{aligned} \quad (72)$$

Otherwise, when

$$\begin{aligned} & I(X_i; X_j X'_i X'_k X_k) + I(X_j; X'_i X'_k X_k) \\ & < \left| |R_i - I(X'_i; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ \right. \\ & \quad \left. - I(X'_i; X'_k | X_k) \right|^+ + \epsilon, \end{aligned} \quad (73)$$

we will show that $P_{r,s}^3(P_{X_1 X_2 X_3 X'_1 X'_3 Y})$ falls doubly exponentially for each $P_{X_1 X_2 X_3 X'_1 X'_3 Y} \in \mathcal{Q}_3$. We upper bound $P_{r,s}^3(P_{X_1 X_2 X_3 X'_1 X'_3 Y})$ by the following set of equations.

$$\begin{aligned} & P_{r,s}^3(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) \\ & = W^n(\mathcal{E}_{r,s,3}(P_{X_1 X_2 X_3 X'_1 X'_3 Y}) | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & \leq \sum_{\substack{(u,w): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w}) \\ \in T_{X_1 X_2 X_3 X'_1 X'_3}^n}} \sum_{\mathbf{y} \in T_{Y | X_1 X_2 X_3 X'_1 X'_3}^n(\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w})} \\ & \quad W^n(\mathbf{y} | \mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3) \\ & \leq \sum_{\substack{(u,w): (\mathbf{x}_{1r}, \mathbf{x}_{2s}, \mathbf{x}_3, \mathbf{x}_{1u}, \mathbf{x}_{3w}) \\ \in T_{X_1 X_2 X_3 X'_1 X'_3}^n}} \exp(-n(I(Y; X'_1 X'_3 | X_1 X_2 X_3) - \epsilon)) \\ & \stackrel{(a)}{=} \exp\left(n\left(\left| |R_1 - I(X'_1; X_1 X_2 X_3)|^+ \right. \right. \right. \\ & \quad \left. \left. \left. + |R_3 - I(X'_3; X_1 X_2 X_3)|^+ - |R_1 - I(X'_1; X'_3 | X_1 X_2 X_3)|^+ \right. \right. \right. \\ & \quad \left. \left. \left. - I(Y; X'_1 X'_3 | X_1 X_2 X_3) + 3\epsilon/2 \right| \right. \right. \right). \end{aligned} \quad (74)$$

where (a) follows from (14). Now, we need to show that (74) goes to zero under the condition given in (73). This is same as the previous analysis of (44) under the condition (49) with R_2 and X'_2 replaced by R_3 and X'_3 . Note that with these replacements, the entire analysis follows through and we obtain the analogues of (56), (57) and (59) as given in (75), (76) and (77) respectively. For

$$\mathcal{P}_2 \stackrel{\text{def}}{=} \{P_{X_1 X_2 X_3 Y} : P_{X_1 X_2 X_3 Y} = P_{X_1} \times Q_{X_2} \times P_{X_3} \times W \text{ for some } Q_{X_2}\}$$

$$R_1 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_2} I(X_1; Y | X_3); \quad (75)$$

$$R_3 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_2} I(X_3; Y | X_1); \quad (76)$$

$$R_1 + R_3 < \min_{P_{X_1 X_2 X_3 Y} \in \mathcal{P}_2} I(X_1 X_3; Y). \quad (77)$$

Similarly, we will obtain rate bounds while analyzing the cases when user 1 and 2 are adversarial.

Thus, for any input distribution $p(x_1)p(x_2)p(x_3)$, we have shown the achievability of the set of rate triples (R_1, R_2, R_3) which, for all permutations (i, j, k) of $(1, 2, 3)$, satisfy the following conditions:

$$R_i < \min_{q(x_k)} I(X_i; Y|X_j), \quad \text{and} \quad (78)$$

$$R_i + R_j < \min_{q(x_k)} I(X_i, X_j; Y), \quad (79)$$

where the mutual information terms are evaluated using the joint distribution $p(x_i)p(x_j)q(x_k)W(y|x_1, x_2, x_3)$.

It remains to argue that the rate region \mathcal{R} given by (9) and (10) is achievable. To this end, consider a distribution¹³ $p_U p_{X_1|U} p_{X_2|U} p_{X_3|U}$. Without loss of generality, take $\mathcal{U} = \{1, 2, \dots, |\mathcal{U}|\}$. It suffices to show the achievability for $p_U(u)$ whose elements are rational numbers. Let l be such that $lp_U(u)$ are integers for all $u \in \mathcal{U}$. For $u \in \mathcal{U}$, let $m_u = lp_U(u)$ and $n_u = \sum_{j \leq u} m_j$, and let $n_0 = 0$.

Consider the l -fold product $W^{\otimes l}$ of the channel W . For this product channel, consider the input distribution $p(\mathbf{x}_1)p(\mathbf{x}_2)p(\mathbf{x}_3)$ defined by

$$p(\mathbf{x}_i) = p((x_{i1}, \dots, x_{il})) = \prod_{u \in \mathcal{U}} \prod_{t=n_{u-1}+1}^{n_u} p_{X_i|U}(x_{it}|u).$$

By (78) and (79) applied to the product channel $W^{\otimes l}$, we may conclude that the rate triple (R_1, R_2, R_3) is achievable for W if, for all permutations (i, j, k) of $(1, 2, 3)$,

$$lR_i \leq \min_{q(\mathbf{x}_k)} I(\mathbf{X}_i; \mathbf{Y}|\mathbf{X}_j), \quad \text{and} \quad (80)$$

$$l(R_i + R_j) \leq \min_{q(\mathbf{x}_k)} I(\mathbf{X}_i, \mathbf{X}_j; \mathbf{Y}). \quad (81)$$

The achievability of the theorem follows from the following observation (for concreteness we take $(i, j, k) = (1, 2, 3)$ below):

$$\begin{aligned} \min_{q(\mathbf{x}_3)} I(\mathbf{X}_1; \mathbf{Y}|\mathbf{X}_2) &= \min_{q(\mathbf{x}_3)} \sum_{t=1}^l I(X_{1t}; \mathbf{Y}|\mathbf{X}_2, X_1^{t-1}) \\ &\stackrel{(a)}{=} \min_{q(\mathbf{x}_3)} \sum_{t=1}^l I(X_{1t}; \mathbf{Y}, X_1^{t-1}|\mathbf{X}_2) \\ &\geq \min_{q(\mathbf{x}_3)} \sum_{t=1}^l I(X_{1t}; Y_t|\mathbf{X}_2) \\ &\geq \sum_{t=1}^l \min_{q(\mathbf{x}_3)} I(X_{1t}; Y_t|\mathbf{X}_2) \\ &\stackrel{(b)}{=} \sum_{t=1}^l \min_{q(x_{3t})} I(X_{1t}; Y_t|X_{2t}) \\ &= \sum_{u \in \mathcal{U}} \sum_{t=n_{u-1}+1}^{n_u} \min_{q(x_{3t})} I(X_{1t}; Y_t|X_{2t}), \end{aligned} \quad (82)$$

where (a) follows from the independence of $X_{11}, X_{12}, \dots, X_{1l}, \mathbf{X}_2$, (b) follows from the memorylessness of the product channel across its components and

¹³For clarity, in the rest of this proof we introduce subscripts to denote the p.m.f.s involved in (9) and (10).

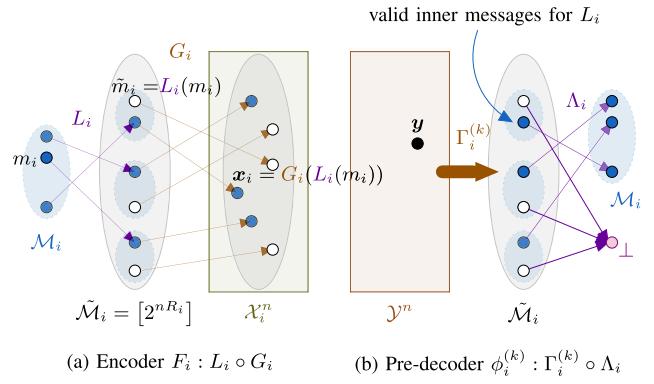


Fig. 14. The encoders and pre-decoders for Theorem 3.

the independence of $X_{21}, X_{22}, \dots, X_{2l}$. Notice that in (82), the $n_u - n_{u-1} = lp_U(u)$ terms in the inner sum corresponding to each $u \in \mathcal{U}$ are identical. For $u \in \mathcal{U}$, let $(X_{1,u}, X_{2,u}, X_{3,u}, Y_u) \sim p_{X_1|U}(\cdot|u) p_{X_2|U}(\cdot|u) q_{X_3|U}(\cdot|u) W(\cdot|\cdot, \cdot, \cdot)$. Then, rewriting (82),

$$\begin{aligned} \min_{q(\mathbf{x}_3)} I(\mathbf{X}_1; \mathbf{Y}|\mathbf{X}_2) &\geq \sum_{u \in \mathcal{U}} (lp_U(u)) \min_{q_{X_3|U}(\cdot|u)} I(X_{1,u}; Y_u|X_{2,u}) \\ &= l \min_{q_{X_3|U}} \sum_{u \in \mathcal{U}} p_U(u) I(X_{1,u}; Y_u|X_{2,u}) \\ &= l \min_{q_{X_3|U}} I(X_1; Y|X_2 U). \end{aligned}$$

Similarly,

$$\min_{q(\mathbf{x}_3)} I(\mathbf{X}_1 \mathbf{X}_2; \mathbf{Y}) \geq l \min_{q_{X_3|U}} I(X_1 X_2; Y|U).$$

Thus, any rate triple satisfying the conditions in (9)-(10) also satisfies (80)-(81) and hence is achievable. \square

B. Randomized Coding Capacity Region

Proof (Achievability of Theorem 3): For each $k = 1, 2, 3$, let $W^{(k)}$ be the 2-user AV-MAC formed by channel inputs from node k as the state and the remaining channel inputs as legitimate inputs. Let (R_1, R_2, R_3) be a rate triple such that, for some $p(u)p(x_1|u)p(x_2|u)p(x_3|u)$, the following conditions hold for all permutations (i, j, k) of $(1, 2, 3)$:

$$R_i < \min_{q(x_k|u)} I(X_i; Y|UX_j), \quad \text{and} \quad (83)$$

$$R_i + R_j < \min_{q(x_k|u)} I(X_i, X_j; Y|U), \quad (84)$$

with the mutual information terms evaluated using the joint distribution $p(u)p(x_1|u)p(x_2|u)q(x_3|u)W(y|x_1, x_2, x_3)$. Note that, by the first part of the direct result of [8, Theorem 1] (see [8, Section III-C]), the rate pair (R_i, R_j) is achievable for the AV-MAC $W^{(k)}$ (see the footnote on page 11). Let $\epsilon > 0$. For each $i \in \{1, 2, 3\}$, let $\tilde{\mathcal{M}}_i = [1 : 2^{nR_i}]$ and $\mathcal{M}_i = [1 : 2^{nR_i}/v]$ for the largest integer $v \leq 3/\epsilon$. In the following, we show the existence of a randomized $(2^{nR_1}/v, 2^{nR_2}/v, 2^{nR_3}/v, n)$ code (F_1, F_2, F_3, ϕ) with P_e^{rand} no larger than ϵ , for sufficiently large n .

1) *Code Design:* We will first describe some randomized maps which will be used in the code design (see Figure 14). For each $i \in \{1, 2, 3\}$, let $G_i : \tilde{\mathcal{M}}_i \rightarrow \mathcal{X}_i^n$ be a randomized map such that it maps $m_i \in \tilde{\mathcal{M}}_i$ to an n -length i.i.d. sequence $G_i(m_i)$ generated according to the distribution p_i . The sequences $G_i(m)$ are independent across $i \in \{1, 2, 3\}$ and $m \in \mathcal{M}_i$. The realization of $G_i(m_i)$ for all $i \in \{1, 2, 3\}$ and $m_i \in \mathcal{M}_i$ is shared with the decoder. For any permutation (i, j, k) of $(1, 2, 3)$, consider the AV-MAC $W^{(k)}$ which corresponds to user- k as the adversary. If we consider $\tilde{\mathcal{M}}_i$ and $\tilde{\mathcal{M}}_j$ as the message sets and G_i and G_j as the corresponding encoders, then this construction ensures that the randomness of the encoders G_i and G_j is private from each other and also private from the adversarial user- k . This joint distribution of G_i and G_j (and the corresponding codewords) is the same as that of the encoders of AV-MAC $W^{(k)}$ in the direct part of [8, Theorem 1, Section III-C]. For G_i and G_j as encoders, let $\Gamma^{(k)}$ denote the decoder corresponding to the decoding sets defined in proof of the direct part of [8, Theorem 1, Section III-C] for the AV-MAC $W^{(k)}$. Suppose $(\Gamma_i^{(k)}, \Gamma_j^{(k)}) := \Gamma^{(k)}$ where $\Gamma_i^{(k)} : \mathcal{Y}^n \rightarrow \tilde{\mathcal{M}}_i$. For all $\epsilon > 0$, by [8, Theorem 1], there exists a large enough n such that for all permutations (i, j, k) of $(1, 2, 3)$, the code $(G_i, G_j, \Gamma^{(k)})$ has error probability no larger than $\epsilon/3$. We consider that n .

For each $i \in \{1, 2, 3\}$, the message set \mathcal{M}_i is randomly embedded into the set $\tilde{\mathcal{M}}_i$ as follows: We choose an arbitrary partition of $\tilde{\mathcal{M}}_i$ into $|\mathcal{M}_i|$ many disjoint equal-sized subsets (each subset size is v). Let us denote the partition by \mathcal{S}_{m_i} , $m_i \in \mathcal{M}_i$ where $\cup_{m_i \in \mathcal{M}_i} \mathcal{S}_{m_i} = \tilde{\mathcal{M}}_i$ and $\mathcal{S}_{m_i} \cap \mathcal{S}_{m'_i} = \emptyset$ for all $m_i, m'_i \in \mathcal{M}_i$ where $m_i \neq m'_i$. The size of each \mathcal{S}_{m_i} , $m_i \in \mathcal{M}_i$ is v ($\leq 3/\epsilon$). The maps $L_i : \mathcal{M}_i \rightarrow \tilde{\mathcal{M}}_i$ and $\Lambda_i : \tilde{\mathcal{M}}_i \rightarrow \mathcal{M}_i$ are the forward and reverse maps for an injection from \mathcal{M}_i to $\tilde{\mathcal{M}}_i$ where, independently for each $m_i \in \mathcal{M}_i$, $L_i(m_i)$ is chosen uniformly at random from \mathcal{S}_{m_i} . Both the encoder maps G_i and L_i are independent for $i = 1, 2, 3$ and are made available to the decoder as the shared secret between user- i and the decoder, unknown to other users.

For each $i \in \{1, 2, 3\}$, the encoder map $F_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$ is defined as $F_i(m_i) = G_i(L_i(m_i))$ for every $m_i \in \mathcal{M}_i$. For $i \in \{1, 2, 3\} \setminus \{i\}$, we define pre-decoder¹⁴

$$\phi_i^{(k)}(\mathbf{y}) := \begin{cases} \Lambda_i(\Gamma_i^{(k)}(\mathbf{y})) & \text{if } \Gamma_i^{(k)}(\mathbf{y}) \in L_i(\mathcal{M}_i), \\ \perp & \text{otherwise.} \end{cases}$$

The decoder $\phi : \mathcal{Y}^n \rightarrow \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{M}_3$ outputs $\phi(\mathbf{y}) = (\hat{m}_1, \hat{m}_2, \hat{m}_3)$, where, for each $i \in \{1, 2, 3\}$ and (j, k) a permutation of $\{1, 2, 3\} \setminus \{i\}$,

$$\hat{m}_i = \begin{cases} \phi_i^{(j)}(\mathbf{y}) & \text{if } \phi_i^{(j)}(\mathbf{y}) = \phi_i^{(k)}(\mathbf{y}) \neq \perp \\ \phi_i^{(j)}(\mathbf{y}) & \text{if } \phi_i^{(j)}(\mathbf{y}) \neq \perp \text{ and } \phi_i^{(k)}(\mathbf{y}) = \perp \\ \phi_i^{(k)}(\mathbf{y}) & \text{if } \phi_i^{(k)}(\mathbf{y}) \neq \perp \text{ and } \phi_i^{(j)}(\mathbf{y}) = \perp \\ 1 & \text{otherwise.} \end{cases}$$

2) *Error Analysis:* We first show that as long as the rate triple (R_1, R_2, R_3) satisfy the constraints (83) and (84), i.e.,

¹⁴In this notation $\phi_i^{(k)}(\mathbf{y})$, we are suppressing the dependence of the pre-decoder (and later the decoder) on the randomness of the encoders.

each pair of rates lie in the corresponding AV-MAC randomized coding capacity region, the following hold simultaneously for every honest user i which sends message $m_i \in \mathcal{M}_i$ and potentially adversarial user $k \neq i$: (i) $\phi_i^{(k)}(\mathbf{Y})$ is m_i w.h.p. (with probability at least $1 - \epsilon/3$) if user- k is indeed adversarial and (ii) $\phi_i^{(k)}(\mathbf{Y})$ is, w.h.p. (with probability at least $1 - \epsilon/3$), either \perp or m_i if user- k is not adversarial. To this end, consider any permutation (i, j, k) of $(1, 2, 3)$ and assume that the adversarial user (if any) is user- k which sends \mathbf{X}_k as its potentially adversarial input to the channel. Suppose, for $(m_i, m_j) \in \mathcal{M}_i \times \mathcal{M}_j$, user- i and user- j send $F_i(m_i)$ and $F_j(m_j)$ respectively. Let \mathbf{Y} denote the channel output.

- (i) First, consider the AV-MAC $W^{(k)}$. Recall that $\Gamma_i^{(k)}(\mathbf{Y}) = L_i(m_i)$ with probability at least $1 - \epsilon/3$. Thus, with probability at least $1 - \epsilon/3$, $\phi_i^{(k)}(\mathbf{Y})$ equals m_i .
- (ii) Next, consider the AV-MAC $W^{(j)}$. In this case, $\Gamma_i^{(j)}(\mathbf{Y})$ may not equal $L_i(m_i)$ as \mathbf{X}_k may not be a valid codeword. We would like to compute $\mathbb{P}(\phi_i^{(j)}(\mathbf{Y}) \notin \{m_i, \perp\})$ where the probability is over $G_i(L_i(m_i))$, $G_j(L_j(m_j))$, \mathbf{X}_k and the channel. Note that G_i and L_i are independent of (potentially jointly distributed and adversarially chosen) G_k , L_k and \mathbf{X}_k . Thus,

$$\begin{aligned} & \mathbb{P}(\phi_i^{(j)}(\mathbf{Y}) \notin \{m_i, \perp\}) \\ &= \mathbb{P}(\Gamma_i^{(j)}(\mathbf{Y}) \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{(j)}(\mathbf{Y}) = \tilde{m}_i, \tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{(j)}(\mathbf{Y}) = \tilde{m}_i) \\ & \quad \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\}) | \Gamma_i^{(j)}(\mathbf{Y}) = \tilde{m}_i) \\ &\stackrel{(a)}{=} \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{(j)}(\mathbf{Y}) = \tilde{m}_i) \\ & \quad \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &\stackrel{(b)}{=} \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{(j)}(\mathbf{Y}) = \tilde{m}_i) \cdot \frac{1}{v} \\ &\leq 1/v \\ &\leq \epsilon/3. \end{aligned}$$

Here, (a) holds as $\Gamma_i^{(j)}(\mathbf{Y}) \perp\!\!\!\perp L_i(\mathcal{M}_i \setminus \{m_i\})$. This is because $L_i(m_i) \perp\!\!\!\perp L_i(\mathcal{M}_i \setminus \{m_i\})$ and $\Gamma_i^{(j)} \perp\!\!\!\perp L_i$ as $\Gamma_i^{(j)}$ is a function of AV-MAC encoders G_i and G_k which are independent of L_i . The equality (b) holds because for $\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}$,

$$\begin{aligned} & \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{m'_i \in \mathcal{M}_i \setminus \{m_i\}} \mathbb{P}(L_i(m'_i) = \tilde{m}_i) \\ &= \sum_{m'_i \in \mathcal{M}_i \setminus \{m_i\}} 1_{\{\tilde{m}_i \in \mathcal{S}_{m'_i}\}} \cdot \frac{1}{v} \\ &= 1/v. \end{aligned}$$

Thus, with probability $1-\epsilon$, for each non-adversarial user i , at least one of the decoders $\phi_i^{(j)}$ or $\phi_i^{(k)}$ outputs the true message while the other decoder outputs either the true message or \perp . \square

Proof (Converse of Theorem 3): We show the converse for the weak adversary. Since, $\mathcal{R}_{\text{random}} \subseteq \mathcal{R}_{\text{random}}^{\text{weak}}$, a converse bound on $\mathcal{R}_{\text{random}}^{\text{weak}}$ is also a converse bound on $\mathcal{R}_{\text{random}}$. Suppose (F_1, F_2, F_3, ϕ) is a $(2^{nR_1}, 2^{nR_2}, 2^{nR_3}, n)$ randomized code such that $P_e^{\text{weak}} \leq \epsilon$ for some $\epsilon > 0$. Recall that F_1, F_2, F_3 are independent. Let $M_i \sim \text{Unif}(\mathcal{M}_i)$, $i = 1, 2, 3$ be independent. Let $\hat{M}_i = \phi_i(\mathbf{Y}, F_1, F_2, F_3)$, $i = 1, 2, 3$. Then, ϵ is an upper bound on (5) which is given by

$$\begin{aligned} P_{e,1}^{\text{weak}} &= \max_{\mathbf{x}_1} \mathbb{P}_{F_2, F_3} \left((\hat{M}_2, \hat{M}_3) \neq (M_2, M_3) \mid \mathbf{X}_1 = \mathbf{x}_1, \right. \\ &\quad \left. \mathbf{X}_2 = F_2(M_2), \mathbf{X}_3 = F_3(M_3) \right) \\ &= \max_{p_{\mathbf{X}_1}} \mathbb{P}_{F_2, F_3} \left((\hat{M}_2, \hat{M}_3) \neq (M_2, M_3) \mid \mathbf{X}_2 = F_2(M_2), \right. \\ &\quad \left. \mathbf{X}_3 = F_3(M_3) \right). \end{aligned}$$

For a vector $\mathbf{x}_j \in \mathcal{X}_j^n$, $j = 1, 2, 3$, we use $x_{j,i}$ to denote its i^{th} index. That is $\mathbf{x}_j = (x_{j,1}, x_{j,2}, \dots, x_{j,n})$. Similarly, a random vector \mathbf{X}_j distributed on \mathcal{X}_j^n can be written as $\mathbf{X}_j = (X_{j,1}, X_{j,2}, \dots, X_{j,n})$. For $i \in [1 : n]$, let $q_{X_{1,i}}$ be some distribution on \mathcal{X}_1 . We consider the following $p_{\mathbf{X}_1}$.

$$p_{\mathbf{X}_1}(\mathbf{x}_1) = \prod_{i=1}^n q_{X_{1,i}}(x_{1,i}).$$

By Fano's inequality, under this $p_{\mathbf{X}_1}$ and when $\mathbf{X}_i = F_i(M_i)$, $i = 2, 3$,

$$H(M_2, M_3 | \mathbf{Y}, F_2, F_3) \leq 1 + n\epsilon(R_2 + R_3).$$

Ignoring small terms, we have

$$\begin{aligned} n(R_2 + R_3) &\leq H(M_2, M_3) \\ &\leq H(M_2, M_3 | F_2, F_3) \\ &\stackrel{(a)}{\approx} I(M_2, M_3; \mathbf{Y} | F_2, F_3) \\ &= \sum_{i=1}^n I(M_2, M_3; Y_i | Y^{i-1}, F_2, F_3) \\ &\leq \sum_{i=1}^n I(M_2, M_3, F_2, F_3, Y^{i-1}; Y_i) \\ &= \sum_{i=1}^n I(M_2, M_3, F_2, F_3, Y^{i-1}, X_{2,i}, X_{3,i}; Y_i) \\ &\stackrel{(b)}{=} \sum_{i=1}^n I(X_{2,i}, X_{3,i}; Y_i), \end{aligned}$$

where (a) follows from Fano's inequality (ignoring an $O(ne)$ term), (b) follows from the memorylessness of the channel and the independence of $X_{1,i}$ over $i = 1, \dots, n$ for the particular $p_{\mathbf{X}_1}$ under consideration.

Let $U \sim \text{Unif}\{1, 2, \dots, n\}$ independent of $(M_1, M_2, M_3, F_1, F_2, F_3, \mathbf{Y})$. We have (where we ignore an additive $O(\epsilon)$ term)

$$R_2 + R_3 \leq I(X_{2,U}, X_{3,U}; Y_U | U).$$

Since, the above bound holds for all $p_{\mathbf{X}_1}(\mathbf{x}_1) = \prod_{i=1}^n q_{X_{1,i}}(x_{1,i})$, and noticing that conditioned on $X_{1,U}, X_{2,U}, X_{3,U}$ the channel law $W_{Y|X_1 X_2 X_3}$ gives the conditional probability of Y_U , we may write

$$R_2 + R_3 \leq \min_{q(x_1|u)} I(X_2, X_3; Y | U) \quad (85)$$

for some $q(x_1|u)$. We note that the distribution of U, X_1, X_2, X_3, Y is $p(u)q(x_1|u)p(x_2|u)p(x_3|u)W_{Y|X_1 X_2 X_3}(y|x_1, x_2, x_3)$ where $p(x_2|u)$ is determined by the distribution of F_2 and $p(x_3|u)$ is determined by the distribution of F_3 .

Proceeding similarly, for $p_{\mathbf{X}_1}(\mathbf{x}_1) = \prod_{i=1}^n q_{X_{1,i}}(x_{1,i})$,

$$\begin{aligned} nR_2 &\leq H(M_2) \\ &\leq H(M_2 | M_3, F_2, F_3) \\ &\approx I(M_2; \mathbf{Y} | M_3, F_2, F_3) \\ &= \sum_{i=1}^n I(M_2; Y_i | Y^{i-1}, M_3, F_2, F_3) \\ &= \sum_{i=1}^n I(M_2, X_{2,i}; Y_i | X_{3,i}, Y^{i-1}, M_3, F_2, F_3) \\ &\leq \sum_{i=1}^n I(X_{2,i}, Y^{i-1}, M_2, M_3, F_2, F_3; Y_i | X_{3,i}) \\ &= \sum_{i=1}^n I(X_{2,i}; Y_i | X_{3,i}). \end{aligned}$$

Hence, we have

$$R_2 \leq \min_{q(x_1|u)} I(X_2; Y | X_3, U), \quad (86)$$

where the joint distribution of the random variables is $p(u)q(x_1|u)p(x_2|u)p(x_3|u)W_{Y|X_1 X_2 X_3}(y|x_1, x_2, x_3)$. We note that $p(u)p(x_2|u)p(x_3|u)$ are the same as in (85). Similarly,

$$R_3 \leq \min_{q(x_2|u)} I(X_3; Y | X_2, U). \quad (87)$$

Similarly, considering $P_{e,2}^{\text{weak}}$ with $p_{\mathbf{X}_2}(x_2^n) = \prod_{i=1}^n q_{X_{2,i}}(x_{2,i})$ (and $\mathbf{X}_i = F_i(W_i)$, $i = 1, 3$), we get

$$R_3 \leq \min_{q(x_2|u)} I(X_3; Y | X_1, U), \quad (88)$$

$$R_1 \leq \min_{q(x_2|u)} I(X_1; Y | X_3, U), \quad (89)$$

$$R_3 + R_1 \leq \min_{q(x_2|u)} I(X_3, X_1; Y | U), \quad (90)$$

where the joint distribution of the random variables is $p(u)p(x_1|u)q(x_2|u)p(x_3|u)W_{Y|X_1 X_2 X_3}(y|x_1, x_2, x_3)$ for some $q_{x_2|u}$. We note that $p(u)$ and $p(x_3|u)$ here are the same as in (85)-(87). Considering $P_{e,3}^{\text{weak}}$ with $p_{\mathbf{X}_3}(x_3^n) = \prod_{i=1}^n q_{X_{3,i}}(x_{3,i})$ (and $\mathbf{X}_i = F_i(W_i)$, $i = 1, 2$), we similarly arrive at

$$R_1 \leq \min_{q(x_3|u)} I(X_1; Y | X_2, U), \quad (91)$$

$$R_2 \leq \min_{q(x_3|u)} I(X_2; Y | X_1, U), \quad (92)$$

$$R_1 + R_2 \leq \min_{q(x_3|u)} I(X_1, X_2; Y | U), \quad (93)$$

where the joint distribution of the random variables is $p(u)p(x_1|u)p(x_2|u)q(x_3|u)W_{Y|X_1X_2X_3}(y|x_1, x_2, x_3)$. The $p(u)$, $p(x_1|u)$, and $p(x_2|u)$ are the same as in (85)–(93). This completes the proof of converse. \square

V. THE k -USER BYZANTINE-MAC

In this section, we generalize our model to a k -user byzantine-MAC for any positive integer k . We allow for a set of users to be controlled by an adversary simultaneously.

We study the problem under both randomized and deterministic codes. The techniques for the 3-user byzantine-MAC are extended to show the characterization of the randomized capacity region. For the deterministic part, we take the first approach (Section I-D2) as mentioned in the introduction. We first show that for any randomized code with vanishing probability of error, there exists another randomized code, also with a vanishing probability of error, which requires only n^2 -valued randomness at each encoder for a code of blocklength n . This argument is along the lines of the extension of the elimination technique [13] provided in [8]. Next, we generalize the symmetrizability conditions to show that the deterministic coding capacity region has non-empty interior if and only if the byzantine-MAC is not symmetrizable. This allows us to use a small rate positive code to share the random bits with the decoder whenever the channel is not symmetrizable and then use the randomized scheme to achieve the entire randomized capacity region under deterministic codes (also see Remark 2).

We give the system model in Section V-A and discuss the randomized and deterministic coding capacity regions in Sections V-B and V-C respectively. We only give proof sketches in these sections and defer the complete proofs to the appendices.

A. System Model

A memoryless k -user byzantine-MAC (W, \mathcal{A}) consists of a k -user memoryless MAC W with input alphabets $\mathcal{X}_1, \mathcal{X}_2, \dots, \mathcal{X}_k$, and output alphabet \mathcal{Y} along with an adversary who can control a set of users simultaneously. The set of users the adversary controls may be any one of the sets in $\mathcal{A} \subseteq 2^{[1:k]}$, where $2^{[1:k]}$ denotes the power set of $[1 : k]$. The other users and the decoder are unaware of the identity of the set \mathcal{Q} of users, $\mathcal{Q} \in \mathcal{A}$, that the adversary controls. In the sequel, we refer to the users in this set $\mathcal{Q} \in \mathcal{A}$ which the adversary controls as the malicious users and the other users as honest. If $\emptyset \in \mathcal{A}$, then it corresponds to the case when all users are honest. For the 3-user byzantine-MAC (Section III) which considers the case when at most one user is malicious, the adversary structure is given by $\mathcal{A} = \{\emptyset, \{1\}, \{2\}, \{3\}\}$. Along the lines of Definition 3 for the three user byzantine-MAC, we define randomized codes for k -user byzantine-MAC (W, \mathcal{A}) below.

Definition 7 (Randomized Code): An $(N_1, N_2, \dots, N_k, n)$ randomized code for the byzantine-MAC (W, \mathcal{A}) consists of the following:

- (i) k message sets, $\mathcal{M}_i = \{1, \dots, N_i\}$, $i = 1, 2, \dots, k$,
- (ii) k independent randomized encoders, $F_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$, where $F_i \sim P_{F_i}$ takes values in $\mathcal{F}_i \subseteq \{g : \mathcal{M}_i \rightarrow \mathcal{X}_i^n\}$, $i = 1, 2, \dots, k$ and

- (iii) a decoder, $\phi : \mathcal{Y}^n \times \mathcal{F}_1 \times \dots \times \mathcal{F}_k \rightarrow \mathcal{M}_1 \times \dots \times \mathcal{M}_k$ where

$$\phi(\mathbf{y}, F_1, \dots, F_k) = (\phi_1(\mathbf{y}, F_1, \dots, F_k), \dots, \phi_k(\mathbf{y}, F_1, \dots, F_k))$$

for some deterministic functions $\phi_i : \mathcal{Y}^n \times \mathcal{F}_1 \times \dots \times \mathcal{F}_k \rightarrow \mathcal{M}_1 \times \dots \times \mathcal{M}_k$, $i = 1, \dots, k$.

Next, we define the probability of error, achievable rate region and the capacity region. As mentioned in Section III-A, the decoder is a function which maps the channel output as well as the random encoding maps to decoded messages. Hence, the adversary can mount an attack by selecting the random encoding maps of the users it controls. Note that while doing this, the adversary does not have access to the random encoding maps of the other (honest) users. Similar to the 3-user case, the adversary selects the encoding maps and chooses the inputs of all malicious users jointly. Note that while doing this, the adversary is unaware of the realizations of the other users' encoding maps. If the adversary controls the users in $\mathcal{Q} \in \mathcal{A}$, then it may choose the encoding maps $f_{\mathcal{Q}}$ (i.e., $(f_i)_{i \in \mathcal{Q}}$) in addition to the input vectors $\mathbf{x}_{\mathcal{Q}}$.

Let $P_{e, \mathcal{Q}}^{\text{rand}}$ denote the average probability of error when the adversary controls the set \mathcal{Q} of users.

$$\begin{aligned} P_{e, \mathcal{Q}}^{\text{rand}} = \max_{\substack{\mathbf{x}_{\mathcal{Q}} \in \mathcal{F}_{\mathcal{Q}} \\ f_{\mathcal{Q}} \in \mathcal{F}_{\mathcal{Q}}}} & \frac{1}{\prod_{i \in \mathcal{Q}^c} N_i} \\ & \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}(\{\phi(\mathbf{Y}, f_{\mathcal{Q}}, F_{\mathcal{Q}^c})_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}\} \\ & \mathbf{X}_{\mathcal{Q}^c} = F_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}, \end{aligned} \quad (94)$$

where $\phi(\mathbf{y}, f_{\mathcal{Q}}, F_{\mathcal{Q}^c})_{\mathcal{Q}^c}$ denotes $\hat{m}_{\mathcal{Q}^c}$ for $\hat{m}_{[1:k]} \in \mathcal{M}_{[1:k]}$ such that $\phi(\mathbf{y}, f_{\mathcal{Q}}, F_{\mathcal{Q}^c}) = \hat{m}_{[1:k]}$. The probability is over independent $F_i \sim P_{F_i}$, $i \in \mathcal{Q}^c$ and the channel.

The average probability of error P_e^{rand} is given by

$$P_e^{\text{rand}} = \max_{\mathcal{Q} \in \mathcal{A}} P_{e, \mathcal{Q}}^{\text{rand}}.$$

Note that though the users controlled by the adversary do not use $f_{\mathcal{Q}}$ for encoding, the decoder uses it and hence its choice gives the adversary additional power. We also emphasize that the decoder is unaware of the identity of the set $\mathcal{Q} \in \mathcal{A}$ of users controlled by the adversary (i.e., in (94), the decoding map ϕ may not depend on \mathcal{Q}).

We say a rate tuple (R_1, R_2, \dots, R_k) is *achievable*, if there is a sequence of $(\lfloor 2^{nR_1} \rfloor, \lfloor 2^{nR_2} \rfloor, \dots, \lfloor 2^{nR_k} \rfloor, n)$ codes $(F_1^{(n)}, F_2^{(n)}, \dots, F_k^{(n)}, \phi^{(n)})_{n=1}^{\infty}$ such that $\lim_{n \rightarrow \infty} P_e^{\text{rand}}(P_{F_1^{(n)}}, P_{F_2^{(n)}}, \dots, P_{F_k^{(n)}}, \phi^{(n)}) \rightarrow 0$. The *randomized coding capacity region* $\mathcal{R}_{\text{random}}$ is the closure of the set of all achievable rate triples.

We also study the *weak* adversary model for the converse where the adversary does not have any knowledge of the any of the random encoding maps while choosing the inputs of the malicious users. Probability of error and capacity region for randomized codes with weak adversary can be defined by

replacing $P_{e,\mathcal{Q}}^{\text{rand}}$ with $P_{e,\mathcal{Q}}^{\text{weak}}$ for $\mathcal{Q} \in \mathcal{A}$ in the above definition, where

$$\begin{aligned} P_{e,\mathcal{Q}}^{\text{weak}} &= \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{\prod_{i \in \mathcal{Q}^c} N_i} \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}\left(\{\phi(\mathbf{Y}, F_{\mathcal{Q}}, F_{\mathcal{Q}^c})_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}\} \mid \mathbf{X}_{\mathcal{Q}^c} = F_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}\right), \end{aligned} \quad (95)$$

The probability is over independent $F_i \sim P_{F_i}$, $i \in [1 : k]$ and the channel.

We denote the *randomized coding capacity region* for the weak adversary by $\mathcal{R}_{\text{random}}^{\text{weak}}$. As was the case in 3-user byzantine-MAC, $\mathcal{R}_{\text{random}} \subseteq \mathcal{R}_{\text{random}}^{\text{weak}}$.

We define deterministic codes for k -user byzantine-MAC (W, \mathcal{A}) along the lines of Definition 1.

Definition 8 (Deterministic code): An $(N_1, N_2, \dots, N_k, n)$ deterministic code for the byzantine-MAC (W, \mathcal{A}) consists of

- (i) k message sets, $\mathcal{M}_i = \{1, \dots, N_i\}$, $i \in \{1, 2, \dots, k\}$,
- (ii) k encoders, $f_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$, $i \in \{1, 2, \dots, k\}$, and
- (iii) a decoder, $\phi : \mathcal{Y}^n \rightarrow \mathcal{M}_1 \times \mathcal{M}_2 \times \dots \times \mathcal{M}_k$.

Let $P_{e,\mathcal{Q}}$ denote the average probability of error when the adversary controls the set $\mathcal{Q} \in \mathcal{A}$ of users.

$$\begin{aligned} P_{e,\mathcal{Q}} &= \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{\prod_{i \in \mathcal{Q}^c} N_i} \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}\left(\{\phi(\mathbf{Y})_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}\} \mid \mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}\right). \end{aligned} \quad (96)$$

The average probability of error P_e is given by

$$P_e = \max_{\mathcal{Q} \in \mathcal{A}} P_{e,\mathcal{Q}}.$$

Similar to the randomized coding case, the decoder is unaware of which set of users from \mathcal{A} are controlled by the adversary.

We say a rate tuple (R_1, R_2, \dots, R_k) is *achievable* if there is a sequence of $(\lfloor 2^{nR_1} \rfloor, \lfloor 2^{nR_2} \rfloor, \dots, \lfloor 2^{nR_k} \rfloor, n)$ codes $(f_1^{(n)}, f_2^{(n)}, \dots, f_k^{(n)}, \phi^{(n)})_{n=1}^{\infty}$ such that $\lim_{n \rightarrow \infty} P_e(f_1^{(n)}, f_2^{(n)}, \dots, f_k^{(n)}, \phi^{(n)}) \rightarrow 0$. The *deterministic coding capacity region* $\mathcal{R}_{\text{deterministic}}$ is the set of all achievable rate tuples.

Recall that for the three user byzantine-MAC (Section III), where the adversary structure is $\mathcal{A} = \{\emptyset, \{1\}, \{2\}, \{3\}\}$, we could show that $P_{e,0} \leq P_{e,1} + P_{e,2} + P_{e,3}$ (see (3)). Generalizing this to the k -user byzantine-MAC (W, \mathcal{A}) , we can show the following lemma whose proof is in Appendix III.

Lemma 6: For any $\mathcal{Q}_1, \dots, \mathcal{Q}_t \in \mathcal{A}$, $t \in \mathbb{N}$ and $\mathcal{Q} \subseteq [1 : k]$ such that $\mathcal{Q} = \cap_{i=1}^t \mathcal{Q}_i$, $P_{e,\mathcal{Q}} \leq \sum_{i=1}^t P_{e,\mathcal{Q}_i}$.

This lemma implies that even if a set $\mathcal{Q} = \cap_{i=1}^t \mathcal{Q}_i$ as in Lemma 6 is removed from \mathcal{A} , the capacity region of a byzantine-MAC remains unchanged.

B. Randomized Coding Capacity Region

Let \mathcal{R} be the closure of the set of all rate tuples (R_1, R_2, \dots, R_k) such that for some $p(u)p(x_1|u)p(x_2|u)\dots p(x_k|u)$, the following conditions hold for all $\mathcal{Q} \in \mathcal{A}$ and $\mathcal{J} \subseteq \mathcal{Q}^c$,

$$\sum_{j \in \mathcal{J}} R_j \leq \min_{q(\mathbf{x}_{\mathcal{Q}}|u)} I(X_{\mathcal{J}}; Y|X_{(\mathcal{Q} \cup \mathcal{J})^c}, U) \quad (97)$$

where the mutual information above is evaluated using the joint distribution $p(u)q(\mathbf{x}_{\mathcal{Q}}|u) \prod_{j \in \mathcal{Q}^c} p(x_j|u)W(y|\mathbf{x}_{\mathcal{Q}}, \mathbf{x}_{\mathcal{Q}^c})$. Here, an upper bound of 2^k on $|\mathcal{U}|$ can be shown using the convex cover method [29, Appendix C].

Remark 3: As discussed after Lemma 6, the capacity region of a byzantine-MAC remains unchanged even if a set $\mathcal{Q} = \cap_{i=1}^t \mathcal{Q}_i$ is removed from \mathcal{A} . It is easy to verify that the rate region \mathcal{R} shares this property. For instance, for the three user case, let $\mathcal{A} = \{\emptyset, \{1\}, \{2\}, \{3\}\}$. Consider the constraint corresponding to $\mathcal{Q} = \emptyset$ and $\mathcal{J} = \{1, 2, 3\}$ in (97)

$$R_1 + R_2 + R_3 \leq I(X_1 X_2 X_3; Y|U).$$

This is implied by the following constraints which correspond to $\mathcal{Q} = \{3\}$, $\mathcal{J} = \{1, 2\}$ and $\mathcal{Q} = \{1\}$, $\mathcal{J} = \{3\}$ respectively

$$\begin{aligned} R_1 + R_2 &\leq \min_{q(x_3|u)} I(X_1 X_2; Y|U) \leq I(X_1 X_2; Y|U) \Big|_{p(x_3|u)}, \\ \text{and } R_3 &\leq \min_{q(x_1|u)} I(X_3; Y|X_2 U) \leq I(X_3; Y|X_2 U) \Big|_{p(x_1|u)}. \end{aligned}$$

Now, the implication follows from

$$\begin{aligned} I(X_1 X_2 X_3; Y|U) &= I(X_1 X_2; Y|U) + I(X_3; Y|X_1 X_2 U) \\ &\stackrel{(a)}{=} I(X_1 X_2; Y|U) + I(X_3; Y X_1|X_2 U) \\ &\geq I(X_1 X_2; Y|U) + I(X_3; Y|X_2 U), \end{aligned}$$

where (a) follows from the conditional independence of X_1, X_2, X_3 given U . Hence, the sum rate constraint (corresponding to \emptyset) is redundant in the three user case.

Theorem 7: For a k -user byzantine-MAC,

$$\mathcal{R}_{\text{random}} = \mathcal{R}_{\text{random}}^{\text{weak}} = \mathcal{R}.$$

Similar to the three user case (Section III-B2), we prove Theorem 7 by showing an achievability in the standard model and a converse for the weak adversary. The converse can be proved by a simple extension of the proof of the converse of Theorem 3 (three-user randomized coding capacity region) and is skipped. The achievability uses arguments similar to the proof of achievability of Theorem 3. It is shown in Appendix IV.

C. Deterministic Coding Capacity Region

Similar to the 3-user case (Section III-B1), we first give a general symmetrizability condition which characterizes the class of channels under which all users cannot communicate reliably in a byzantine-MAC (W, \mathcal{A}) using deterministic codes. For the 3-user byzantine-MAC case, this condition (given below) specializes to the three conditions (6)-(8).

Definition 9 (Symmetrizability and symmetrizable byzantine-MAC): For a non-empty set $\mathcal{T} \subseteq [1 : k]$, we say that a byzantine-MAC (W, \mathcal{A}) is \mathcal{T} -symmetrizable if there exist sets $\mathcal{Q}, \mathcal{Q}' \in \mathcal{A}$, not necessarily distinct, satisfying $\mathcal{Q} \cap \mathcal{T} = \mathcal{Q}' \cap \mathcal{T} = \emptyset$, and a pair of conditional distributions $P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}^{\text{I}}$ and $P'_{X_{\mathcal{Q}'}|X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}^{\text{I}}$ such that

$$\begin{aligned} \sum_{x'_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}} P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}(x'_{\mathcal{Q}}|x_{\mathcal{T}}, x_{\mathcal{Q} \setminus \mathcal{Q}'}) \\ W(y|x'_{\mathcal{Q}}, \tilde{x}_{\mathcal{T}}, x_{\mathcal{Q}' \setminus \mathcal{Q}}, x_{(\mathcal{T} \cup \mathcal{Q} \cup \mathcal{Q}')^c}) \end{aligned}$$

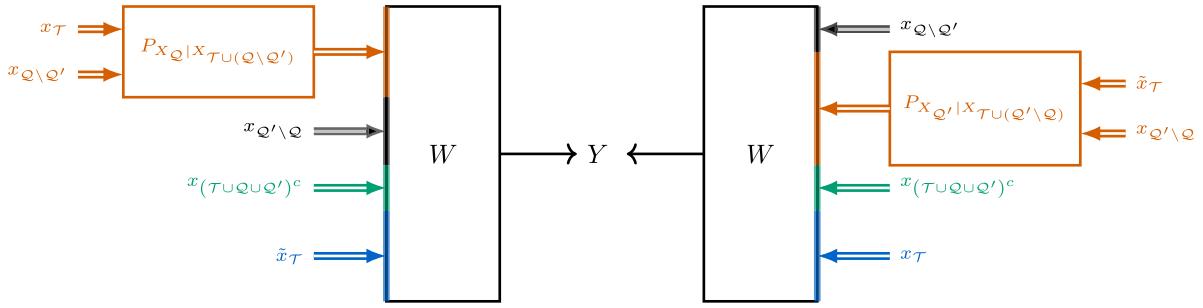


Fig. 15. For each $(\tilde{x}_T, x_T, x_{Q \setminus Q'}, x_{Q' \setminus Q}, x_{(\tau \cup Q \cup Q')^c})$, the conditional output distributions in the two cases above are the same. Thus, the receiver is unable to tell whether the users in set \mathcal{T} are sending \tilde{x}_T or x_T .

$$= \sum_{\tilde{x}_{Q'} \in \mathcal{X}_{Q'}} P'_{X_{Q'} | X_{\tau \cup (Q' \setminus Q)}}(\tilde{x}_{Q'} | \tilde{x}_T, x_{Q' \setminus Q}) \\ W(y | \tilde{x}_{Q'}, x_T, x_{Q \setminus Q'}, x_{(\tau \cup Q \cup Q')^c}) \quad (98)$$

for all $x_T, \tilde{x}_T \in \mathcal{X}_T$, $x_{Q \setminus Q'} \in \mathcal{X}_{Q \setminus Q'}$, $x_{Q' \setminus Q} \in \mathcal{X}_{Q' \setminus Q}$, $x_{(\tau \cup Q \cup Q')^c} \in \mathcal{X}_{(\tau \cup Q \cup Q')^c}$ and $y \in \mathcal{Y}$. We say that a byzantine-MAC (W, \mathcal{A}) is **symmetrizable** if it is \mathcal{T} -symmetrizable for any $\mathcal{T} \neq \emptyset$.

Fig. 15 illustrates the symmetrizable condition in (98). The set \mathcal{T} of users are being symmetrized by the users in sets $\mathcal{Q}, \mathcal{Q}' \in \mathcal{A}$. The users not in $\mathcal{T} \cup \mathcal{Q} \cup \mathcal{Q}'$ are not symmetrized. Definition 9 extends the notion of symmetrizable for the three users case (Definition 5) to the k -user byzantine-MAC with adversary structure \mathcal{A} . It generalizes the three conditions (6)-(8) to a single condition given by (98). In particular, $\mathcal{T} = \{j, k\}$ and $\mathcal{Q} = \mathcal{Q}' = \{i\}$ recovers (6), $\mathcal{T} = \{k\}$ and $\mathcal{Q} = \mathcal{Q}' = \{i\}$ recovers (7), and $\mathcal{T} = \{k\}$, $\mathcal{Q} = \{i\}$ and $\mathcal{Q}' = \{j\}$ recovers (8). Now, we are ready to state our main result.

Theorem 8: For a k user byzantine-MAC (W, \mathcal{A}) , the interior of the deterministic coding capacity region, $\text{int}(\mathcal{R}_{\text{deterministic}})$ is empty if and only if it is symmetrizable. Furthermore, when (W, \mathcal{A}) is not symmetrizable, $\mathcal{R}_{\text{deterministic}} = \mathcal{R}_{\text{random}}$.

Proof Sketch: For the *converse*, similar to the 3-user case, we show in Appendix VIII that if the channel is symmetrizable then $\text{int}(\mathcal{R}_{\text{deterministic}}) = \emptyset$. When the channel is not symmetrizable, the outer bound on the rate region follows from Theorem 7. To show the *achievability* direction of the theorem, *i.e.*, $\mathcal{R}_{\text{deterministic}} \supseteq \mathcal{R}_{\text{random}}$ if (W, \mathcal{A}) is not symmetrizable, we take the first approach discussed in the introduction (Section I-D2). We first show the following lemma (proved in Appendix VII) which states that all users can communicate at positive rates if a byzantine-MAC is not symmetrizable.

Lemma 9: If a k -user byzantine-MAC (W, \mathcal{A}) is not symmetrizable, then there exists $(R_1, R_2, \dots, R_k) \in \mathcal{R}_{\text{deterministic}}$ where $R_i > 0$ for all $i \in [1 : k]$.

Next, we show that for every randomized code achieving a small probability of error, there exists another randomized code which also achieves a small probability of error, but requires only n^2 -valued randomness at each encoder for a code of blocklength n . This *randomness reduction* argument is along the lines of the extension of the elimination technique [13] given in Jahn [8, Theorem 1]. The formal statement and its proof is given in Appendix V.

The achievability of Theorem 8 is done in two phases. In the first phase, each user communicates a small number of their uniformly distributed message bits using the positive rate deterministic codes given by Lemma 9. These will serve as the shared random bits between the user and the receiver in the second phase. The first phase is short compared to the second phase and only needs to communicate $\log n^2$ bits for a second phase of blocklength n . In the second phase, this small amount of randomness will be used by the new code obtained from the randomness reduction argument to communicate the remaining message bits. Note that the first phase allows the adversary to maliciously choose inputs of the users they control and thus the shared randomness between the malicious users and the decoder. This is why in our model, we allow the adversary to select the encoding maps for all users in \mathcal{Q} .

The above argument is formalized in Lemma 10 below and is proved in Appendix VI. Its proof is along the lines of the proof of [28, Theorem 12.11].

Lemma 10: For a byzantine-MAC, if there exists $(R_1, R_2, \dots, R_k) \in \mathcal{R}_{\text{deterministic}}$ where $R_i > 0$ for all $i \in [1 : k]$, then $\mathcal{R}_{\text{deterministic}} \supseteq \mathcal{R}_{\text{random}}$. \square

Similar to the 3-user case, the proof of Lemma 9 (formally given in Appendix VII) employs a codebook generated using a random coding argument (see Lemma 15 in Appendix VII) and is along the lines of [10, Lemma 2] and [22, Lemma 3]. The decoder is a generalization of 3-user decoder given in Definition 6 and is defined below.

Definition 10 (Decoder): For $\eta > 0$, and encoding maps, $f_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$ for $i \in [1 : k]$, the decoding set $\mathcal{D}_{m_1, m_2, \dots, m_k} \subseteq \mathcal{Y}^n$ of the message tuple $(m_1, m_2, \dots, m_k) \in \mathcal{M}_1 \times \mathcal{M}_2 \times \dots \times \mathcal{M}_k$ is defined as the intersection of the sets $\mathcal{D}_{m_i}^{(i)}$, $i \in [1 : k]$, *i.e.*, $\mathcal{D}_{m_1, m_2, \dots, m_k} \stackrel{\text{def}}{=} \bigcap_{i=1}^k \mathcal{D}_{m_i}^{(i)}$, where the sets $\mathcal{D}_{m_i}^{(i)}$, $i \in [1 : k]$ are defined as follows:

A sequence $\mathbf{y} \in \mathcal{D}_{m_i}^{(i)}$, $i \in [1 : k]$, if there exists $\mathcal{Q} \in \mathcal{A}$, $i \notin \mathcal{Q}$, $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$, $\tilde{m}_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}$ where $\tilde{m}_i = m_i$ and random variables $X_{\mathcal{Q}^c}, X_{\mathcal{Q}}$ and Y with $(f_{\mathcal{Q}^c}(\tilde{m}_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}, \mathbf{y}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y}^n$, satisfying the following:

- 1) $D(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} || (\prod_{i \in \mathcal{Q}^c} P_{X_i}) P_{X_{\mathcal{Q}}} W) < \eta$.
- 2) Suppose there exist $\mathcal{Q}' \in \mathcal{A}$, not necessarily distinct from \mathcal{Q} , a non-empty set $\mathcal{T} \subseteq (\mathcal{Q} \cup \mathcal{Q}')^c$ with $i \in \mathcal{T}$, $\mathbf{x}'_{\mathcal{Q}'} \in \mathcal{X}_{\mathcal{Q}'}^n$, $m'_{\mathcal{Q} \setminus \mathcal{Q}'} \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}$, $m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}$ such that $m'_t \neq \tilde{m}_t$ for all $t \in \mathcal{T}$ such that for the joint distribution $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q}'} X'_{\mathcal{Q} \setminus \mathcal{Q}'} Y}$ defined

$$\begin{aligned} & \text{by } (f_{\mathcal{Q}^c}(\tilde{m}_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}, f_{\mathcal{T}}(m'_{\mathcal{T}}), f_{\mathcal{Q} \setminus \mathcal{Q}'}(m'_{\mathcal{Q} \setminus \mathcal{Q}'}), \mathbf{x}'_{\mathcal{Q}'}, \mathbf{y}) \in \\ & T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}, Y}^n, \\ & D(P_{X'_{\mathcal{Q} \setminus \mathcal{Q}'} X_{\mathcal{Q}^c} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus (\mathcal{T} \cup \mathcal{Q}')} X'_{\mathcal{Q}'}, Y} || (\prod_{t \in \mathcal{T}} P_{X'_t})(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}'} P_{X'_j}) \\ & (\prod_{l \in \mathcal{Q}^c \setminus (\mathcal{T} \cup \mathcal{Q}')} P_{X_l}) P_{X'_{\mathcal{Q}'}, W}) < \eta. \end{aligned} \quad (99)$$

Then,

$$I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} | X_{\mathcal{Q}}) < \eta. \quad (100)$$

In the definition of $\mathcal{D}_{m_i}^{(i)}$ above, condition 1 checks for typicality with respect to channel inputs $(f_j(\tilde{m}_j), j \in \mathcal{Q}^c)$ and $\mathbf{x}_{\mathcal{Q}}$. Under condition (99), where an alternative input to the channel $(f_t(m'_t), t \in \mathcal{T})$, $(f_j(m'_j), j \in \mathcal{Q} \setminus \mathcal{Q}')$, $(f_l(m_l), l \in \mathcal{Q}^c \setminus (\mathcal{T} \cup \mathcal{Q}'))$ and $\mathbf{x}'_{\mathcal{Q}'}$ looks typical, condition (100) implies that the input $(f_j(\tilde{m}_j), j \in \mathcal{Q}^c)$ and $\mathbf{x}_{\mathcal{Q}}$ is a more plausible explanation for the channel output than the alternative input (see Fig. 15).

As mentioned earlier, Definition 10 is a generalization of 3-user decoder in Definition 6. In particular, check (a) can be obtained by setting $\mathcal{Q} = \mathcal{Q}' = \{3\}$ and $\mathcal{T} = \{1, 2\}$, (b) by setting $\mathcal{Q} = \mathcal{Q}' = \{3\}$ and $\mathcal{T} = \{1\}$ and (c) by setting $\mathcal{Q} = \{3\}$, $\mathcal{Q}' = \{2\}$ and $\mathcal{T} = \{1\}$.

Similar to Lemma 2, we can show that for small enough $\eta > 0$, $\mathcal{D}_{m_1, m_2, \dots, m_k} \cap \mathcal{D}_{\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_k} = \emptyset$ for every $(m_1, m_2, \dots, m_k) \neq (\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_k)$. See Lemma 17 in Appendix VII for the formal statement and proof.

APPENDIX I PROOF OF LEMMA 2

Proof: Suppose $\mathbf{y} \in \mathcal{Y}^n$ is such that $\mathbf{y} \in \mathcal{D}_{m_1}^{(1)} \cap \mathcal{D}_{\tilde{m}_1}^{(1)}$ for $m_1, \tilde{m}_1 \in \mathcal{M}_1$ where $\tilde{m}_1 \neq m_1$. Then there exist permutations (i, j) and (\tilde{i}, \tilde{j}) of $(2, 3)$ such that one of the following cases holds.

Case 1: $(\tilde{i}, \tilde{j}) = (i, j)$ There exist $m_j, \tilde{m}_j \in \mathcal{M}_j$, sequences $\mathbf{x}_i, \tilde{\mathbf{x}}_i \in \mathcal{X}_i^n$, and random variables $X_1, \tilde{X}_1, X_j, \tilde{X}_j, X_i, \tilde{X}_i$ with $(f_1(m_1), f_1(\tilde{m}_1), f_j(m_j), f_j(\tilde{m}_j), \mathbf{x}_i, \tilde{\mathbf{x}}_i) \in T_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i \tilde{X}_i}^n$ such that $D(P_{X_1 X_j X_i Y} || P_{X_1} \times P_{X_j} \times P_{X_i} \times W), D(P_{\tilde{X}_1 \tilde{X}_j \tilde{X}_i Y} || P_{\tilde{X}_1} \times P_{\tilde{X}_j} \times P_{\tilde{X}_i} \times W) < \eta$ and

Case 1(a) if $\tilde{m}_j \neq m_j$, then $I(X_1 X_j Y; \tilde{X}_1 \tilde{X}_j | X_i), I(\tilde{X}_1 \tilde{X}_j Y; X_1 X_j | \tilde{X}_i) < \eta$.

Case 1(b) if $\tilde{m}_j = m_j$, then $\tilde{X}_j = X_j$ and $I(X_1 X_j Y; X_1 | X_i), I(\tilde{X}_1 \tilde{X}_j Y; X_1 | \tilde{X}_i) < \eta$.

Case 2: $(\tilde{i}, \tilde{j}) = (j, i)$

There exist $m_j \in \mathcal{M}_j$, $\tilde{m}_i \in \mathcal{M}_i$, sequences $\tilde{\mathbf{x}}_j \in \mathcal{X}_j^n$, $\mathbf{x}_i \in \mathcal{X}_i^n$ and random variables $X_1, \tilde{X}_1, X_j, \tilde{X}_j, X_i, \tilde{X}_i$ with $(f_1(m_1), f_1(\tilde{m}_1), f_j(m_j), \tilde{\mathbf{x}}_j, \mathbf{x}_i, f_i(\tilde{m}_i)) \in T_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i \tilde{X}_i}^n$ such that $D(P_{X_1 X_j X_i Y} || P_{X_1} \times P_{X_j} \times P_{X_i} \times W), D(P_{\tilde{X}_1 \tilde{X}_j \tilde{X}_i Y} || P_{\tilde{X}_1} \times P_{\tilde{X}_j} \times P_{\tilde{X}_i} \times W) < \eta$ and $I(X_1 X_j Y; X_1 \tilde{X}_i | X_i), I(\tilde{X}_1 \tilde{X}_j Y; X_1 X_j | \tilde{X}_i) < \eta$.

We first analyze **Case 1(a)**. Let $W_{Y|X_1 X_j X_i}$ be denoted by W .

$$\begin{aligned} & D(P_{X_1 X_j X_i Y} || P_{X_1} \times P_{X_j} \times P_{X_i} \times W) \\ & + D(P_{\tilde{X}_1 \tilde{X}_j} || P_{\tilde{X}_1} \times P_{\tilde{X}_j}) \end{aligned}$$

$$\begin{aligned} & + I(X_1 X_j Y; \tilde{X}_1 \tilde{X}_j | X_i) \\ & \stackrel{(a)}{=} \sum_{x_1, x_j, x_i, y} P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y) \\ & \log \frac{P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y)}{P_{X_1}(x_1) P_{X_j}(x_j) P_{X_i}(x_i) W(y|x_1, x_j, x_i)} \\ & + \sum_{\tilde{x}_1, \tilde{x}_j} P_{\tilde{X}_1 \tilde{X}_j}(\tilde{x}_1, \tilde{x}_j) \log \frac{P_{\tilde{X}_1 \tilde{X}_j}(\tilde{x}_1, \tilde{x}_j)}{P_{\tilde{X}_1}(\tilde{x}_1) P_{\tilde{X}_j}(\tilde{x}_j)} \\ & + \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y} P_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i Y}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y) \\ & \log \frac{P_{X_1 \tilde{X}_1 X_j \tilde{X}_j Y|X_i}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y)}{P_{X_1 X_j Y|X_i}(x_1, x_j, y|x_i) P_{\tilde{X}_1 \tilde{X}_j|X_i}(\tilde{x}_1, \tilde{x}_j|x_i) W(y|x_1, x_j, x_i)} \\ & = \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y} P_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i Y}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y) \\ & \log \frac{P_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i Y}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, x_i, y)}{P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) P_{\tilde{X}_j}(\tilde{x}_j) P_{X_i}(x_i) W(y|x_1, x_j, x_i)} \\ & = D(P_{X_1 \tilde{X}_1 X_j \tilde{X}_j X_i Y} || P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{\tilde{X}_j} P_{X_i} | \tilde{X}_1 \tilde{X}_j W) \\ & \stackrel{(b)}{\geq} D(P_{X_1 \tilde{X}_1 X_j \tilde{X}_j Y} || P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{\tilde{X}_j} \tilde{V}_1) \\ & \quad \text{where } \tilde{V}_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) \\ & = \sum_{x_i} P_{X_i | \tilde{X}_1 \tilde{X}_j}(x_i | \tilde{x}_1, \tilde{x}_j) W(y|x_1, x_j, x_i), \end{aligned}$$

where (b) follows from the log sum inequality. From the given conditions, we know that the term on the LHS of (a) is no greater than 3η . Thus, $D(P_{X_1 \tilde{X}_1 X_j \tilde{X}_j Y} || P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{\tilde{X}_j} \tilde{V}_1) \leq 3\eta$. Using Pinsker's inequality, it follows that

$$\begin{aligned} 3\eta & \geq D(P_{\tilde{X}_1 \tilde{X}_j \tilde{X}_i Y} || P_{\tilde{X}_1} \times P_{\tilde{X}_j} \times P_{\tilde{X}_i} \times W) \\ & + D(P_{X_1 X_j} || P_{X_1} \times P_{X_j}) \\ & + I(\tilde{X}_1 \tilde{X}_j Y; X_1 X_j | \tilde{X}_i) \\ & \geq D(P_{X_1 \tilde{X}_1 X_j \tilde{X}_i Y} || P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{\tilde{X}_i} V_1) \text{ where} \\ V_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) & = \sum_{\tilde{x}_i} P_{\tilde{X}_i | X_1 X_j}(\tilde{x}_i | x_1, x_j) W(y | \tilde{x}_1, \tilde{x}_j, \tilde{x}_i). \end{aligned} \quad (101)$$

Using Pinsker's inequality, it follows that

$$\begin{aligned} & \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, y} \left| P_{X_1 \tilde{X}_1 X_j \tilde{X}_i Y}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, y) - \right. \\ & \left. P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) P_{\tilde{X}_i}(\tilde{x}_i) V_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) \right| \\ & \leq c\sqrt{3\eta}, \end{aligned} \quad (102)$$

From (101) and (102),

$$\sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, y} P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) P_{\tilde{X}_i}(\tilde{x}_i)$$

$$\left| \tilde{V}_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) - V_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) \right| \leq 2c\sqrt{3\eta}.$$

This implies that

$$\begin{aligned} \max_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, y} & \left| \tilde{V}_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) - V_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) \right| \\ & \leq \frac{2c\sqrt{3\eta}}{\alpha^4}. \end{aligned} \quad (103)$$

Similar to [10, (A.15) on page 748], since $W_{Y|X_1 X_2 X_3}$ is not $\mathcal{X}_1 \times \mathcal{X}_j$ -symmetrizable by \mathcal{X}_i (i.e., (6) does not hold for $(i, j, k) = (i, j, 1)$), we can show that for any pair of channels $P_{\tilde{X}_i|X_1 X_j}$ and $P_{X_i|\tilde{X}_1 \tilde{X}_j}$, there exists $\zeta_1 > 0$ such that

$$\max_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, y} \left| \tilde{V}_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) - V_1(y|x_1, \tilde{x}_1, x_j, \tilde{x}_j) \right| \geq \zeta_1.$$

This contradicts (103) if $\eta < \frac{\zeta_1^2 \alpha^8}{12c^2}$.

We now analyze **Case 1(b)**.

$$\begin{aligned} & D(P_{X_1 X_j X_i Y} \| P_{X_1} \times P_{X_j} \times P_{X_i} \times W) \\ & \quad + I(X_1 X_j Y; \tilde{X}_1 | X_i) \\ & \stackrel{(a)}{=} \sum_{x_1, x_j, x_i, y} P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y) \\ & \quad \log \frac{P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y)}{P_{X_1}(x_1) P_{X_j}(x_j) P_{X_i}(x_i) W(y|x_1, x_j, x_i)} \\ & \quad + \sum_{x_1, \tilde{x}_1, x_j, x_i, y} P_{X_1 \tilde{X}_1 X_j X_i Y}(x_1, \tilde{x}_1, x_j, x_i, y) \\ & \quad \log \frac{P_{X_1 \tilde{X}_1 X_j Y|X_i}(x_1, \tilde{x}_1, x_j, y|x_i)}{P_{X_1 X_j Y|X_i}(x_1, x_j, y|x_i) P_{\tilde{X}_1|X_i}(\tilde{x}_1|x_i)} \\ & = \sum_{x_1, \tilde{x}_1, x_j, x_i, y} P_{X_1 \tilde{X}_1 X_j X_i Y}(x_1, \tilde{x}_1, x_j, x_i, y) \\ & \quad \log \frac{P_{X_1 \tilde{X}_1 X_j X_i Y}(x_1, \tilde{x}_1, x_j, x_i, y)}{P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) P_{X_i|\tilde{X}_1}(x_i|\tilde{x}_1) W(y|x_1, x_j, x_i)} \\ & = D(P_{X_1 \tilde{X}_1 X_j X_i Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{X_i|\tilde{X}_1} W) \\ & \stackrel{(b)}{\geq} D(P_{X_1 \tilde{X}_1 X_j Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} \tilde{V}_2) \end{aligned}$$

where $\tilde{V}_2(y|x_1, \tilde{x}_1, x_j) = \sum_{x_i} P_{X_i|\tilde{X}_1}(x_i|\tilde{x}_1) W(y|x_1, x_j, x_i)$,

where (b) follows from the log sum inequality. From the given conditions, we know that the term on the LHS of (a) is no greater than 2η . Thus, $D(P_{X_1 \tilde{X}_1 X_j Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} \tilde{V}_2) \leq 2\eta$. Using Pinsker's inequality, it follows that

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, y} & \left| P_{X_1 \tilde{X}_1 X_j Y}(x_1, \tilde{x}_1, x_j, y) - \right. \\ & \left. P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) \tilde{V}_2(y|x_1, \tilde{x}_1, x_j) \right| \\ & \leq c\sqrt{2\eta}, \end{aligned} \quad (104)$$

where c is some positive constant. Following a similar line of argument, we can show that

$$\begin{aligned} 2\eta & \geq D(P_{\tilde{X}_1 X_j \tilde{X}_i Y} \| P_{\tilde{X}_1} \times P_{X_j} \times P_{\tilde{X}_i} \times W) \\ & \quad + I(\tilde{X}_1 X_j Y; X_i | \tilde{X}_i) \\ & \geq D(P_{X_1 \tilde{X}_1 X_j Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} V_2) \text{ where} \end{aligned}$$

$$V_2(y|x_1, \tilde{x}_1, x_j) = \sum_{\tilde{x}_i} P_{\tilde{X}_i|X_1}(\tilde{x}_i|x_1) W(y|\tilde{x}_1, x_j, \tilde{x}_i).$$

Using Pinsker's inequality, it follows that

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, y} & \left| P_{X_1 \tilde{X}_1 X_j Y}(x_1, \tilde{x}_1, x_j, y) - \right. \\ & \left. P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) V_2(y|x_1, \tilde{x}_1, x_j) \right| \\ & \leq c\sqrt{3\eta}. \end{aligned} \quad (105)$$

From (104) and (105),

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, y} & P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) \\ & \left| \tilde{V}_2(y|x_1, \tilde{x}_1, x_j) - V_2(y|x_1, \tilde{x}_1, x_j) \right| \leq 2c\sqrt{3\eta}. \end{aligned}$$

This implies that

$$\max_{x_1, \tilde{x}_1, x_j, y} \left| \tilde{V}_2(y|x_1, \tilde{x}_1, x_j) - V_2(y|x_1, \tilde{x}_1, x_j) \right| \leq \frac{2c\sqrt{2\eta}}{\alpha^4}. \quad (106)$$

Similar to [10, (A.5) on page 747], since $W_{Y|X_1 X_2 X_3}$ is not $\mathcal{X}_1 \times \mathcal{X}_j$ -symmetrizable by \mathcal{X}_i (i.e., (7) does not hold for $(i, j, k) = (i, j, 1)$), we can show that for any pair of channels $P_{\tilde{X}_i|X_1}$ and $P_{X_i|\tilde{X}_1}$, there exists $\zeta_2 > 0$ such that

$$\max_{x_1, \tilde{x}_1, x_j, y} \left| \tilde{V}_2(y|x_1, \tilde{x}_1, x_j) - V_2(y|x_1, \tilde{x}_1, x_j) \right| \geq \zeta_2.$$

This contradicts (106) if $\eta < \frac{\zeta_2^2 \alpha^8}{8c^2}$.

We now analyse **Case 2**.

$$\begin{aligned} & D(P_{X_1 X_j X_i Y} \| P_{X_1} \times P_{X_j} \times P_{X_i} \times W) \\ & \quad + D(P_{\tilde{X}_1, \tilde{X}_i} \| P_{\tilde{X}_1} \times P_{\tilde{X}_i}) \\ & \quad + I(X_1 X_j Y; \tilde{X}_1 \tilde{X}_i | X_i) \\ & \stackrel{(a)}{=} \sum_{x_1, x_j, x_i, y} P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y) \\ & \quad \log \frac{P_{X_1 X_j X_i Y}(x_1, x_j, x_i, y)}{P_{X_1}(x_1) P_{X_j}(x_j) P_{X_i}(x_i) W(y|x_1, x_j, x_i)} \\ & \quad + \sum_{\tilde{x}_1, \tilde{x}_i} P_{\tilde{X}_1 \tilde{X}_i}(\tilde{x}_1, \tilde{x}_i) \\ & \quad \log \frac{P_{\tilde{X}_1 \tilde{X}_i}(\tilde{x}_1, \tilde{x}_i)}{P_{\tilde{X}_1}(\tilde{x}_1) P_{\tilde{X}_i}(\tilde{x}_i)} \\ & \quad + \sum_{x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y} P_{X_1 \tilde{X}_1 X_j X_i Y}(x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y) \\ & \quad \log \frac{P_{X_1 \tilde{X}_1 X_j X_i Y}(x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y|x_i)}{P_{\tilde{X}_1 \tilde{X}_i|X_i}(\tilde{x}_1, \tilde{x}_i|x_i) P_{X_1 X_j Y|X_i}(x_1, x_j, y|x_i)} \\ & = \sum_{x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y} P_{X_1 \tilde{X}_1 X_j X_i \tilde{X}_i Y}(x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y) \\ & \quad \log \frac{P_{X_1 \tilde{X}_1 X_j X_i \tilde{X}_i Y}(x_1, \tilde{x}_1, x_j, x_i, \tilde{x}_i, y)}{P_{X_1}(x_1) P_{\tilde{X}_1}(\tilde{x}_1) P_{X_j}(x_j) P_{X_i}(\tilde{x}_i) P_{\tilde{X}_i}(\tilde{x}_i) W(y|x_1, x_j, x_i, \tilde{x}_i)} \\ & = D(P_{X_1 \tilde{X}_1 X_j X_i \tilde{X}_i Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{X_i} P_{\tilde{X}_i} W) \\ & \stackrel{(b)}{\geq} D(P_{X_1 \tilde{X}_1 X_j X_i Y} \| P_{X_1} P_{\tilde{X}_1} P_{X_j} P_{X_i} \tilde{V}_3) \text{ where} \end{aligned}$$

$$\tilde{V}_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) = \sum_{x_i} P_{X_i|\tilde{X}_1\tilde{X}_i}(x_i|\tilde{x}_1, \tilde{x}_i) W(y|x_1, x_j, x_i),$$

where (b) follows from the log sum inequality. From the given conditions, we know that the term on the LHS of (a) is no greater than 3η . Thus, $D(P_{X_1\tilde{X}_1X_j\tilde{X}_iY}||P_{X_1}P_{\tilde{X}_1}P_{X_j}P_{\tilde{X}_i}V_3) \leq 3\eta$. Using Pinsker's inequality, it follows that

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_i, y} & \left| P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(x_1, \tilde{x}_1, x_j, \tilde{x}_i, y) - \right. \\ & \left. P_{X_1}(x_1)P_{\tilde{X}_1}(\tilde{x}_1)P_{X_j}(x_j)P_{\tilde{X}_i}(\tilde{x}_i)\tilde{V}_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) \right| \\ & \leq c\sqrt{3\eta} \end{aligned} \quad (107)$$

for some constant $c > 0$. Following a similar line of argument,

$$\begin{aligned} & D(P_{\tilde{X}_1\tilde{X}_j\tilde{X}_iY}||P_{\tilde{X}_1} \times P_{\tilde{X}_j} \times P_{\tilde{X}_i} \times W) \\ & + D(P_{X_1X_j}||P_{X_1} \times P_{X_j}) \\ & + I(\tilde{X}_1\tilde{X}_iY; X_1X_j|\tilde{X}_j) \\ & \stackrel{(a)}{=} \sum_{\tilde{x}_1, \tilde{x}_j, \tilde{x}_i, y} P_{\tilde{X}_1\tilde{X}_j\tilde{X}_iY}(\tilde{x}_1, \tilde{x}_j, \tilde{x}_i, y) \\ & \log \frac{P_{\tilde{X}_1\tilde{X}_j\tilde{X}_iY}(\tilde{x}_1, \tilde{x}_j, \tilde{x}_i, y)}{P_{\tilde{X}_1}(\tilde{x}_1)P_{\tilde{X}_j}(\tilde{x}_j)P_{\tilde{X}_i}(\tilde{x}_i)W(y|\tilde{x}_1, \tilde{x}_j, \tilde{x}_i)} \\ & + \sum_{x_1, x_j} P_{X_1X_j}(x_1, x_j) \log \frac{P_{X_1X_j}(x_1, x_j)}{P_{X_1}(x_1)P_{X_j}(x_j)} \\ & + \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, \tilde{x}_i, y} P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, \tilde{x}_i, y) \\ & \log \frac{P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(\tilde{x}_1, x_1, x_j, \tilde{x}_j, \tilde{x}_i, y|\tilde{x}_j)}{P_{\tilde{X}_1\tilde{X}_iY}(\tilde{x}_1, \tilde{x}_i, y|\tilde{x}_j)P_{X_1X_j|\tilde{X}_j}(x_1, x_j|\tilde{x}_j)} \\ & = \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_j, \tilde{x}_i, y} P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, \tilde{x}_i, y) \\ & \log \frac{P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(x_1, \tilde{x}_1, x_j, \tilde{x}_j, \tilde{x}_i, y)}{P_{X_1}(x_1)P_{\tilde{X}_1}(\tilde{x}_1)P_{X_j}(x_j)P_{\tilde{X}_i}(\tilde{x}_i)P_{\tilde{X}_j|\tilde{X}_1X_j}(\tilde{x}_j|x_1, x_j)W(y|\tilde{x}_1, \tilde{x}_j, \tilde{x}_i)} \\ & = D(P_{X_1\tilde{X}_1X_j\tilde{X}_iY}||P_{X_1}P_{\tilde{X}_1}P_{X_j}P_{\tilde{X}_i}P_{\tilde{X}_j|\tilde{X}_1X_j}W) \\ & \geq D(P_{X_1\tilde{X}_1X_j\tilde{X}_iY}||P_{X_1}P_{\tilde{X}_1}P_{X_j}P_{\tilde{X}_i}V_3) \text{ where} \end{aligned}$$

$$V_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) = \sum_{\tilde{x}_j} P_{\tilde{X}_j|X_1X_j}(\tilde{x}_j|x_1, x_j) W(y|\tilde{x}_1, \tilde{x}_j, \tilde{x}_i).$$

From the given conditions, the term on the left of (a) is no larger than 3η . Thus, $D(P_{X_1\tilde{X}_1X_j\tilde{X}_iY}||P_{X_1}P_{\tilde{X}_1}P_{X_j}P_{\tilde{X}_i}V_3) \leq 3\eta$.

Using Pinsker's inequality, it follows that

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_i, y} & \left| P_{X_1\tilde{X}_1X_j\tilde{X}_iY}(x_1, \tilde{x}_1, x_j, \tilde{x}_i, y) - \right. \\ & \left. P_{X_1}(x_1)P_{\tilde{X}_1}(\tilde{x}_1)P_{X_j}(x_j)P_{\tilde{X}_i}(\tilde{x}_i)V_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) \right| \\ & \leq c\sqrt{3\eta}. \end{aligned} \quad (108)$$

From (107) and (108),

$$\begin{aligned} \sum_{x_1, \tilde{x}_1, x_j, \tilde{x}_i, y} & P_{X_1}(x_1)P_{\tilde{X}_1}(\tilde{x}_1)P_{X_j}(x_j)P_{\tilde{X}_i}(\tilde{x}_i) \\ & \left| \tilde{V}_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) - V_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) \right| \\ & \leq 2c\sqrt{3\eta}. \end{aligned} \quad (109)$$

This implies that

$$\max_{x_1, \tilde{x}_1, x_j, \tilde{x}_i, y} \left| \tilde{V}_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) - V_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) \right| \leq \frac{2c\sqrt{3\eta}}{\alpha^4}. \quad (110)$$

Since $W_{Y|X_1X_2X_3}$ is not \mathcal{X}_1 -symmetrizable by $\mathcal{X}_j/\mathcal{X}_i$ (i.e., (8) does not hold for $(i, j, k) = (i, j, 1)$), for any pair of channels $P_{X_i|\tilde{X}_1\tilde{X}_i}$ and $P_{\tilde{X}_j|X_1X_j}$, there exists $\zeta_3 > 0$, such that

$$\max_{x_1, \tilde{x}_1, x_j, \tilde{x}_i, y} \left| \tilde{V}_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) - V_3(y|x_1, \tilde{x}_1, x_j, \tilde{x}_i) \right| \geq \zeta_3.$$

This contradicts (110) if $\eta < \frac{\zeta_3^2 \alpha^8}{12c^2}$. Let $\zeta \stackrel{\text{def}}{=} \min\{\zeta_1, \zeta_2, \zeta_3\}$, any η satisfying $0 < \eta < \frac{\zeta^2 \alpha^8}{12c^2}$ ensures disjoint decoding regions. \square

APPENDIX II PROOF OF LEMMA 4 (CODEBOOK LEMMA)

To prove Lemma 4, we will first define some terminology and prove a concentration result in Lemma 11. This will be used to prove Lemma 4 (Codebook Lemma) as a corollary.

A. A Concentration Result

In this subsection, we restate [24, Theorem 2.1] in a form that can be directly used for proving the properties of the codebook.

For a positive integer b , let \mathcal{S}_b denote the symmetric group of degree b , i.e., it contains the permutations of $\{1, 2, \dots, b\}$. For a permutation $\sigma \in \mathcal{S}_b$, let $\sigma(i)$, $i \in \{1, 2, \dots, b\}$ denote the image of i under σ . Let \mathcal{A} be a set. For a b -length tuple $(\alpha_1, \dots, \alpha_b)$ consisting of distinct elements of \mathcal{A} , let

$$\mathcal{H}_{(\alpha_1, \dots, \alpha_b)} = \left\{ a \in (\{\alpha_1, \dots, \alpha_b\} \cup \{*\})^b : \exists \sigma \in \mathcal{S}_b \text{ such that for all } j \in [1 : b] \text{ if } a_j \neq * \text{ then } a_j = \alpha_{\sigma(j)} \right\},$$

where a_j represents the j^{th} element of the tuple a . For $a \in \mathcal{H}_{(\alpha_1, \dots, \alpha_b)}$, let $|a| = |\{i : a_i \neq *\}|$. For a tuple $(\gamma_1, \dots, \gamma_b)$ consisting of distinct elements of \mathcal{A} , we say that $a \in \mathcal{H}_{(\alpha_1, \dots, \alpha_b)}$ and $(\gamma_1, \dots, \gamma_b)$ are $(\alpha_1, \dots, \alpha_b)$ -compatible (denoted by $(\gamma_1, \dots, \gamma_b) \sim [a, (\alpha_1, \dots, \alpha_b)]$), if for all $l \in \{1, \dots, b\}$,

$$\gamma_l = a_l, \quad \text{if } a_l \neq *, \\ \gamma_l \in \mathcal{A} \setminus \{\alpha_1, \dots, \alpha_b\}, \quad \text{otherwise.}$$

For example, let $\mathcal{A} = \{1, 2, \dots, 9\}$, $b = 5$, $(\alpha_1, \dots, \alpha_b) = (1, 2, 3, 4, 5)$ and $a = (1, 2, *, *, 4)$. Then, $a \in \mathcal{H}_{(\alpha_1, \dots, \alpha_b)}$ with $|a| = 3$. Suppose $(\gamma_1, \dots, \gamma_b) = (1, 2, 6, 8, 4)$. Then, $(\gamma_1, \dots, \gamma_b) \sim [a, (\alpha_1, \dots, \alpha_b)]$.

Lemma 11: For an index set \mathcal{I} , let $\{Y_i : i \in \mathcal{I}\}$ be a set of independent random variables. Let β be a positive integer. Let $\mathcal{J} \subseteq \mathcal{I}^\beta$ be a set of β length tuples consisting of distinct elements from \mathcal{I} . For $(i_1, \dots, i_\beta) \in \mathcal{J}$, let $V_{(i_1, \dots, i_\beta)}$ be a binary random variable which is a function of $Y_{i_1}, \dots, Y_{i_\beta}$. Suppose $U = \sum_{(i_1, \dots, i_\beta) \in \mathcal{J}} V_{(i_1, \dots, i_\beta)}$. Let E be defined as given in (111), shown at the bottom of the next page.

For $\gamma > 0$, $\nu > 1$ if there exists $\delta_1, \delta_2, \dots, \delta_\beta > 1$ such that for all $i \in [1 : \beta]$, $\frac{1}{(2\beta)^\beta} \left(\frac{\delta_{i-1}-1}{2\gamma} E - \beta! \right) > \delta_i E$ for $\delta_0 := \nu$, then

$$\mathbb{P}(U \geq \nu E) \leq (|\mathcal{I}| \beta + 1)^{\beta^2} e^{-\gamma/3}. \quad (112)$$

Proof: For $(i_1, \dots, i_\beta) \in \mathcal{J}$, let

$$\tilde{U}_{(i_1, \dots, i_\beta)} = \sum_{(j_1, \dots, j_\beta) \in \mathcal{J}: \{j_1, \dots, j_\beta\} \cap \{i_1, \dots, i_\beta\} \neq \emptyset} V_{(j_1, \dots, j_\beta)}.$$

To show (112), we will first show that

$$\mathbb{P}(U \geq \nu E) \leq e^{-\gamma/3} + \sum_{(i_1, \dots, i_\beta) \in \mathcal{J}} \mathbb{P} \left(\tilde{U}_{(i_1, \dots, i_\beta)} > \frac{(\nu - 1)E}{2\gamma} \right) \quad (113)$$

using [24, Theorem 2.1], which is restated below.

Lemma 1: [24, Theorem 2.1] Suppose that $Y_\alpha, \alpha \in \mathcal{A}$, is a finite family of non-negative random variables and that \sim is a symmetric relation on the index set \mathcal{A} such that each Y_α is independent of $\{Y_\beta : \beta \sim \alpha\}$; in other words, the pairs (α, β) with $\alpha \sim \beta$ define the edge set of a (weak) dependency graph for the variables Y_α . Let $X := \sum_\alpha Y_\alpha$ and $\mu := \mathbb{E}X = \sum_\alpha \mathbb{E}Y$. Let further, for $\alpha \in \mathcal{A}$, $\tilde{X}_\alpha := \sum_{\beta \sim \alpha} Y_\beta$. If $t \geq \mu > 0$, then for every real $r > 0$,

$$\mathbb{P}(X > \mu + t) \leq e^{-r/3} + \sum_{\alpha \in \mathcal{A}} \mathbb{P} \left(\tilde{X}_\alpha > \frac{t}{2r} \right).$$

In order to obtain (113) from [24, Theorem 2.1], we use \mathcal{J} in place of \mathcal{A} and $V_{(i_1, \dots, i_\beta)}$ in place of Y_α . We note that every $(i_1, \dots, i_\beta), (j_1, \dots, j_\beta) \in \mathcal{J}$ such that $\{i_1, \dots, i_\beta\} \cap \{j_1, \dots, j_\beta\} \neq \emptyset$, $(i_1, \dots, i_\beta) \sim (j_1, \dots, j_\beta)$ as per the symmetric relation given in [24, Theorem 2.1]. Thus, the definitions of $\tilde{U}_{(i_1, \dots, i_\beta)}$ and \tilde{X}_α are consistent. We upper bound the LHS of (113) as follows:

$$\begin{aligned} \mathbb{P}(X \geq \nu E) &= \mathbb{P}(X - \mathbb{E}[X] \geq \nu E - \mathbb{E}[X]) \\ &\leq \mathbb{P}(X - \mathbb{E}[X] \geq \nu E - E) \\ &= \mathbb{P}(X - \mathbb{E}[X] \geq (\nu - 1)E) \end{aligned}$$

Theorem [24, Theorem 2.1] is applied on $\mathbb{P}(X \geq \mathbb{E}[X] + (\nu - 1)E)$ with $(\nu - 1)E$ as t and γ as r .

Now, we will show (112). We will use **strong induction** on β . When $\beta = 1$, (113) implies $\mathbb{P}(U \geq \nu E) \leq e^{-\gamma/3}$. This is because for any 1-length tuple $(i) \in \mathcal{J}$, $\tilde{U}_{(i)} = V_{(i)}$, which, being a binary random variable, is at most 1. However, $\frac{1}{(2\beta)^\beta} \left(\frac{\nu-1}{2\gamma} E - \beta! \right) > \delta_1 E \geq 0$ implies that for $\beta = 1$, $\frac{1}{2} \left(\frac{\nu-1}{2\gamma} E - 1 \right) > 0$. Therefore, $\frac{\nu-1}{2\gamma} E > 1$ and the second term on the RHS of (113) is zero. Thus, (112) holds for $\beta = 1$.

Now, for the **induction hypothesis**, consider any $\beta' \leq k$ for some positive integer k . For an index set \mathcal{I}' , let $\{Y'_i : i \in \mathcal{I}'\}$ be a set of independent random variables. Let $\mathcal{J}' \subseteq \mathcal{I}'^{\beta'}$ be a set of β' -length tuples consisting of distinct elements from \mathcal{I}' . For $(i_1, \dots, i_{\beta'}) \in \mathcal{J}'$, let $V'_{(i_1, \dots, i_{\beta'})}$ be a binary random variable which is a function of $Y'_{i_1}, Y'_{i_2}, \dots, Y'_{i_{\beta'}}$. Suppose $U' = \sum_{(i_1, \dots, i_{\beta'}) \in \mathcal{J}'} V'_{(i_1, \dots, i_{\beta'})}$. Suppose

Let

$$\begin{aligned} E' &\geq \max \left\{ \max_{(i_1, \dots, i_{\beta'}) \in \mathcal{J}'} \max_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{\beta'})} \\ 1 \leq |a| \leq \beta' - 1}} \left(\sum_{(j_1, \dots, j_{\beta'}) \in \mathcal{J}': (j_1, \dots, j_{\beta'}) \sim [a, (i_1, \dots, i_{\beta'})]} V'_{(j_1, \dots, j_{\beta'})} \right) \right. \\ &\quad \left. \mathbb{E} \left[\left(Y'_{i_1}, \dots, Y'_{i_{\beta'}} \right) = \left(y'_{i_1}, \dots, y'_{i_{\beta'}} \right) \right] \right], \mathbb{E}[U'] \right\}, \end{aligned}$$

For $\gamma' > 0$, $\nu' > 1$, if there exists $\delta'_1, \delta'_2, \dots, \delta'_{\beta'} > 1$ such that for all $i \in [1 : \beta']$, $\frac{1}{(2\beta')^{\beta'}} \left(\frac{\delta'_{i-1}-1}{2\gamma'} E' - \beta'! \right) > \delta'_i E'$ for $\delta'_0 := \nu'$, then

$$\mathbb{P}(U' \geq \nu' E') \leq (|\mathcal{I}'| \beta' + 1)^{\beta'^2} e^{-\gamma'/3}.$$

Now, for $\beta = k + 1$ and any γ, ν , and E and random variables satisfying the conditions in Lemma 11, (113) gives

$$\mathbb{P}(U \geq \nu E) \leq e^{-\gamma/3} + \sum_{(i_1, \dots, i_{k+1}) \in \mathcal{J}} \mathbb{P} \left(\tilde{U}_{(i_1, \dots, i_{k+1})} > \frac{(\nu - 1)E}{2\gamma} \right).$$

For $(i_1, \dots, i_{k+1}) \in \mathcal{J}$, and any realization $(y_{i_1}, \dots, y_{i_{k+1}})$ of $(Y_{i_1}, \dots, Y_{i_{k+1}})$, consider the steps in (114)–(116), shown at the next page. There, (a) holds because $\sum_{\sigma \in \mathcal{S}} V_{\sigma(i_1, \dots, i_{k+1})}$, being a sum of binary random variables, takes the maximum value $|\mathcal{S}|$ which is $(k+1)!$. The equality (b) holds because $\mathbb{P} \left(\sum_{1 \leq i \leq t} A_i > c \right) \leq \mathbb{P} \left(\bigcup_{1 \leq i \leq t} \{A_i > c/t\} \right)$ for any integer t , real number c and random variables A_1, \dots, A_t . The inequality (c) uses union bound and the fact that $|\mathcal{H}_{(i_1, \dots, i_{k+1})}| \leq (\# \text{ of subsets of } \{i_1, \dots, i_{k+1}\}) \times |\mathcal{S}_{k+1}|$. Thus, $|\mathcal{H}_{(i_1, \dots, i_{k+1})}| \leq 2^{k+1}(k+1)! \leq (2(k+1))^{k+1}$. Inequality (d) holds because $E \geq 1$ and (e) follows from the conditions on ν, γ and $\beta = k+1$ in the statement of Lemma 11.

Fix $(i_1, \dots, i_{k+1}) \in \mathcal{J}$, $(Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}})$ and $a \in \mathcal{H}_{(i_1, \dots, i_{k+1})}$ such that $|a| = l$ where $l \in [1 : k]$. We will use induction hypothesis at this stage. To use induction hypothesis, choose $\nu' = \delta_1$, $\gamma' = \gamma$,

$$E \geq \max \left\{ \max_{(i_1, \dots, i_\beta) \in \mathcal{J}} \left(\max_{\substack{(y_{i_1}, \dots, y_{i_\beta}), \\ a \in \mathcal{H}_{(i_1, \dots, i_\beta)} \\ 1 \leq |a| \leq \beta - 1}} \mathbb{E} \left[\left. \sum_{(j_1, \dots, j_\beta) \in \mathcal{J}: (j_1, \dots, j_\beta) \sim [a, (i_1, \dots, i_\beta)]} V_{(j_1, \dots, j_\beta)} \right| (Y_{i_1}, \dots, Y_{i_\beta}) = (y_{i_1}, \dots, y_{i_\beta}) \right] \right), \mathbb{E}[U] \right\} \quad (111)$$

$$\begin{aligned}
& \mathbb{P} \left(\tilde{U}_{(i_1, \dots, i_{k+1})} > \frac{(\nu-1)E}{2\gamma} \mid (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \leq \mathbb{P} \left(\sum_{\sigma \in \mathcal{S}_{k+1}} V_{\sigma(i_1, \dots, i_{k+1})} + \sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{(\nu-1)E}{2\gamma} \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \quad (114)
\end{aligned}$$

$$\begin{aligned}
& = \mathbb{P} \left(\sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{(\nu-1)E}{2\gamma} - \sum_{\sigma \in \mathcal{S}_{k+1}} V_{\sigma(i_1, \dots, i_{k+1})} \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \quad (115)
\end{aligned}$$

$$\begin{aligned}
& \stackrel{(a)}{\leq} \mathbb{P} \left(\sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{(\nu-1)E}{2\gamma} - |\mathcal{S}_{k+1}| \mid (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \stackrel{(b)}{\leq} \mathbb{P} \left(\bigcup_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{1}{|\mathcal{H}_{(i_1, \dots, i_{k+1})}| - 1 - (k+1)!} \left(\frac{(\nu-1)E}{2\gamma} - (k+1)! \right) \right) \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \leq \mathbb{P} \left(\bigcup_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{1}{|\mathcal{H}_{(i_1, \dots, i_{k+1})}|} \left(\frac{(\nu-1)E}{2\gamma} - (k+1)! \right) \right) \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \stackrel{(c)}{\leq} \sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \mathbb{P} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{1}{(2(k+1))^{k+1}} \left(\frac{(\nu-1)E}{2\gamma} - (k+1)! \right) \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \stackrel{(d)}{\leq} \sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \mathbb{P} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \frac{1}{(2(k+1))^{k+1}} \left(\frac{(\nu-1)E}{2\gamma} - (k+1)!E \right) \mid \right. \\
& \quad \left. (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right) \\
& \stackrel{(e)}{\leq} \sum_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \mathbb{P} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \delta_1 E \mid (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right). \quad (116)
\end{aligned}$$

$E' = E$, $\beta' = k+1-l$ and $\mathcal{I}' = \mathcal{I} \setminus \{i_1, \dots, i_{k+1}\}$. The set of random variables $\{Y'_i : i \in \mathcal{I}'\}$ is given by $Y'_i = Y_i, \forall i \in \mathcal{I}'$. For $i \in [1 : k+1]$, let $|a_1^{i-1}| = |\{j \in [1 : i-1] : a_j \neq *\}|$. The set \mathcal{J}' consists of $(k+1-l)$ -length tuples of distinct elements from \mathcal{I}' such that for every $(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'$, there exists $(m_1, \dots, m_{k+1}) \in \mathcal{J}$ such that $m_l = a_l$ if $a_l \neq *$. Else, $m_l = j_{l-|a_1^{l-1}|}$. For such $(m_1, \dots, m_{k+1}) \in \mathcal{J}$ and (j_1, \dots, j_{k+1-l}) , we will say that $(j_1, \dots, j_{k+1-l}) + a = (m_1, \dots, m_{k+1})$. Thus, for every $(m_1, \dots, m_{k+1}) \in \mathcal{J}$ such that $(m_1, \dots, m_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]$, there exists a unique $(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'$ with $(j_1, \dots, j_{k+1-l}) + a = (m_1, \dots, m_{k+1})$.

For $(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'$, the binary random variable $V'_{(j_1, \dots, j_{k+1-l})}$ is the random variable $V_{(m_1, \dots, m_{k+1})}$ where $(m_1, \dots, m_{k+1}) = (j_1, \dots, j_{k+1-l}) + a$ and the random variables $(Y_{i_1}, \dots, Y_{i_{k+1}})$ are fixed to $(y_{i_1}, \dots, y_{i_{k+1}})$. For $U' = \sum_{(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'} V'_{(j_1, \dots, j_{k+1-l})}$, we will use induction hypothesis on $\mathbb{P}(U' \geq \delta_1 E)$.

$$\begin{aligned} & \mathbb{P}(U' \geq \delta_1 E) \\ &= \mathbb{P}\left(\sum_{(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'} V'_{(j_1, \dots, j_{k+1-l})} > \delta_1 E\right) \\ &= \mathbb{P}\left(\sum_{\substack{(m_1, \dots, m_{k+1}) \in \mathcal{J}: \\ (m_1, \dots, m_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(m_1, \dots, m_{k+1})} > \delta_1 E \right. \\ &\quad \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right). \quad (117) \end{aligned}$$

We know that

$$\begin{aligned} E &\geq \max \left\{ \max_{\substack{(y_{i_1}, \dots, y_{i_{k+1}}) \in \mathcal{J} \\ (i_1, \dots, i_{k+1}) \in \mathcal{I}}} \max_{\substack{a \in \mathcal{H}_{(i_1, \dots, i_{k+1})} \\ 1 \leq |a| \leq k}} \right. \\ &\quad \left. \mathbb{E}\left[\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} \right. \right. \\ &\quad \left. \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right], \mathbb{E}[U] \right\}, \end{aligned}$$

and for $\gamma > 0$, $\nu > 1$ there exists $\delta_1, \delta_2, \dots, \delta_{k+1}$ such that for all $i \in [1 : k+1]$, $\delta_i > 1$ and for $\delta_0 = \nu$, $\frac{1}{(2(k+1))^{k+1}} \left(\frac{\delta_{i-1}-1}{2\gamma} E - (k+1)! \right) > \delta_i E$.

We will use this to show that the choices of γ' , ν' , E' , β' satisfy the conditions in the induction hypothesis.

$$\begin{aligned} \mathbb{E}[U'] &= \mathbb{E}\left[\sum_{(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'} V'_{(j_1, \dots, j_{k+1-l})} \right] \\ &= \mathbb{E}\left[\sum_{\substack{(m_1, \dots, m_{k+1}) \in \mathcal{J}: \\ (m_1, \dots, m_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(m_1, \dots, m_{k+1})} \right. \\ &\quad \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right] \\ &\leq E = E' \end{aligned}$$

For $(j_1, \dots, j_{k+1-l}) \in \mathcal{J}'$, $a' \in \mathcal{H}_{(j_1, \dots, j_{k+1-l})}$ with $|a'| = l'$ for $1 \leq l' \leq k-l$, define a $(k+1)$ -length tuple a'' as

$$a''_l = \begin{cases} a_l, & \text{if } a_l \neq *, \\ a'_{l-|a_1^{l-1}|}, & \text{if } a_l = *. \end{cases}$$

for all $l \in [1 : k+1]$. Let $(m_1, \dots, m_{k+1}) \in \mathcal{J}$ be such that $(j_1, \dots, j_{k+1-l}) + a = (m_1, \dots, m_{k+1})$. Then, for fixed $(y_{j_1}, \dots, y_{j_{k+1-l}})$,

$$\begin{aligned} & \mathbb{E}\left[\sum_{\substack{(g_1, \dots, g_{k+1-l}) \in \mathcal{J}': \\ (g_1, \dots, g_{k+1-l}) \sim [a', (j_1, \dots, j_{k+1-l})]}} V'_{(g_1, \dots, g_{k+1-l})} \right. \\ &\quad \left. \left| (Y_{j_1}, \dots, Y_{j_{k+1-l}}) = (y_{j_1}, \dots, y_{j_{k+1-l}}) \right. \right] \\ &= \mathbb{E}\left[\sum_{\substack{(h_1, \dots, h_{k+1}) \in \mathcal{J}: \\ (h_1, \dots, h_{k+1}) \sim [a'', (m_1, \dots, m_{k+1})]}} V_{(h_1, \dots, h_{k+1})} \right. \\ &\quad \left. \left| \begin{array}{l} (Y_{j_1}, \dots, Y_{j_{k+1-l}}) = (y_{j_1}, \dots, y_{j_{k+1-l}}), \\ (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \end{array} \right. \right] \\ &\stackrel{(a)}{=} \mathbb{E}\left[\sum_{\substack{(h_1, \dots, h_{k+1}) \in \mathcal{J}: \\ (h_1, \dots, h_{k+1}) \sim [a'', (m_1, \dots, m_{k+1})]}} V_{(h_1, \dots, h_{k+1})} \right. \\ &\quad \left. \left| (Y_{m_1}, \dots, Y_{m_{k+1}}) = (y_{m_1}, \dots, y_{m_{k+1}}) \right. \right] \\ &\leq E = E'. \end{aligned}$$

In the above, (a) follows from definition of \mathcal{J}' and \mathcal{J} .

Now, we need to show that for $\nu' = \delta'_0 = \delta_1$, $\gamma' = \gamma$, there exists $\delta'_1, \delta'_2, \dots, \delta'_{\beta'}$ such that for all $i \in [1 : \beta']$, $\delta'_i > 1$ and $\frac{1}{(2\beta')^{\beta'}} \left(\frac{\delta'_{i-1}-1}{2\gamma'} E' - \beta'! \right) > \delta'_i E'$. First note that as $l \in [1 : k]$, $\beta' \in [1 : k]$. We know that there exists $\delta_1, \delta_2, \dots, \delta_{k+1}$ such that for all $i \in [1 : k+1]$, $\delta_i > 1$ and for $\delta_0 = \nu$, $\frac{1}{(2(k+1))^{k+1}} \left(\frac{\delta_{i-1}-1}{2\gamma} E - (k+1)! \right) > \delta_i E$. Let $\delta'_i = \delta_{i+1}$ for all $i \in [1 : \beta']$. Then, for all $i \in [1 : \beta']$, $\delta'_i > 1$ and

$$\begin{aligned} & \frac{1}{(2\beta')^{\beta'}} \left(\frac{\delta'_{i-1}-1}{2\gamma'} E' - (\beta')! \right) \\ &= \frac{1}{(2\beta')^{\beta'}} \left(\frac{\delta_i-1}{2\gamma} E - (\beta')! \right) \\ &\geq \frac{1}{(2(k+1))^{k+1}} \left(\frac{\delta_i-1}{2\gamma} E - (k+1)! \right) \\ &\geq \delta_{i+1} E \\ &= \delta'_i E'. \end{aligned}$$

With this, all the conditions in the induction hypothesis are satisfied and we are ready to apply induction hypothesis. Thus,

$$\begin{aligned} & \mathbb{P}\left(\sum_{\substack{(m_1, \dots, m_{k+1}) \in \mathcal{J}: \\ (m_1, \dots, m_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(m_1, \dots, m_{k+1})} > \delta_1 E \right. \\ &\quad \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right) \end{aligned}$$

$$\begin{aligned} &\stackrel{(a)}{=} \mathbb{P}(U' \geq \delta_1 E) \\ &= (|\mathcal{I}|(k+1-l)+1)^{(k+1-l)^2} e^{-\gamma/3}, \end{aligned} \quad (118)$$

where (a) uses (117). Continuing the analysis of (116),

$$\begin{aligned} &\sum_{\substack{a \in \mathcal{H} \\ 1 \leq |a| \leq k}} \mathbb{P} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \delta_1 E \right. \\ &\quad \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right) \\ &= \sum_{l=1}^k \sum_{\substack{a \in \mathcal{H} \\ |a|=l}} \mathbb{P} \left(\sum_{\substack{(j_1, \dots, j_{k+1}) \in \mathcal{J}: \\ (j_1, \dots, j_{k+1}) \sim [a, (i_1, \dots, i_{k+1})]}} V_{(j_1, \dots, j_{k+1})} > \delta_1 E \right. \\ &\quad \left. \left| (Y_{i_1}, \dots, Y_{i_{k+1}}) = (y_{i_1}, \dots, y_{i_{k+1}}) \right. \right) \\ &\stackrel{(b)}{\leq} \sum_{l=1}^k \sum_{\substack{a \in \mathcal{H} \\ |a|=l}} (|\mathcal{I}|(k+1-l)+1)^{(k+1-l)^2} e^{-\gamma/3} \\ &= \sum_{l=1}^k \binom{k+1}{l} \binom{k+1}{l} l! (|\mathcal{I}|(k+1-l)+1)^{(k+1-l)^2} e^{-\gamma/3} \\ &\stackrel{(c)}{=} \sum_{m=1}^k \binom{k+1}{k+1-m} \binom{k+1}{k+1-m} (k+1-m)! \\ &\quad (|\mathcal{I}|m+1)^{m^2} e^{-\gamma/3} \\ &= \sum_{m=1}^k \binom{k+1}{k+1-m} \frac{(k+1)!}{m!} (|\mathcal{I}|m+1)^{m^2} e^{-\gamma/3} \\ &\leq \sum_{m=1}^k \binom{k+1}{m} ((k+1)!) (|\mathcal{I}|k+1)^{km} e^{-\gamma/3} \\ &\leq \sum_{m=0}^{k+1} \binom{k+1}{m} ((k+1)!) (|\mathcal{I}|k+1)^{km} e^{-\gamma/3} \\ &= (k+1)! e^{-\gamma/3} \sum_{m=0}^{k+1} \binom{k+1}{m} ((|\mathcal{I}|k+1)^k)^m \\ &\leq (k+1)! e^{-\gamma/3} \left((|\mathcal{I}|k+1)^k + 1 \right)^{k+1} \\ &\leq (k+1)^{(k+1)} e^{-\gamma/3} ((|\mathcal{I}|k+1)+1)^{k(k+1)} \end{aligned}$$

Inequality (b) uses (118). The equality (c) is obtained by substituting l with $k+1-m$.

Thus, using this analysis, we see that for $\beta = k+1$,

$$\begin{aligned} \mathbb{P}(U \geq \nu E) &\leq e^{-\gamma/3} \\ &\quad + \sum_{(i_1, \dots, i_{k+1}) \in \mathcal{J}} \mathbb{P} \left(\tilde{U}_{(i_1, \dots, i_{k+1})} > \frac{(\nu-1)E}{2\gamma} \right) \\ &\leq e^{-\gamma/3} \\ &\quad + \sum_{(i_1, \dots, i_{k+1}) \in \mathcal{J}} (k+1)^{(k+1)} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &= e^{-\gamma/3} + |\mathcal{J}|(k+1)^{(k+1)} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &\leq e^{-\gamma/3} + |\mathcal{I}|^{k+1} (k+1)^{(k+1)} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \end{aligned}$$

$$\begin{aligned} &\leq e^{-\gamma/3} + (|\mathcal{I}|(k+1))^{k+1} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &\leq (|\mathcal{I}|(k+1)+1)^{k(k+1)} e^{-\gamma/3} \\ &\quad + (|\mathcal{I}|(k+1))^{k+1} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &\leq ((|\mathcal{I}|(k+1))^{k+1} + 1) e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &\leq (|\mathcal{I}|(k+1)+1)^{k+1} e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{k(k+1)} \\ &\leq e^{-\gamma/3} (|\mathcal{I}|(k+1)+1)^{(k+1)(k+1)}. \end{aligned}$$

□

B. Preliminary Codebook Lemma

We use the concentration result from Section II-A (Lemma 11) to prove the existence of a codebook with properties as given in Lemma 12. Roughly speaking, each property counts the number of codewords which are typical with fixed vectors. The codebook lemma (Lemma 4) follows from Lemma 12 as a corollary. We first state and prove Lemma 12 and give a proof of Lemma 4 in the next subsection. We need to define the terminology of *Total Correlation* to state the properties of the codebook in Lemma 12. For random variables Z_1, Z_2, \dots, Z_m , let $C(Z_1; Z_2; \dots; Z_m)$ denote the *total correlation* of the random variables Z_1, Z_2, \dots, Z_m which is given by

$$C(Z_1; Z_2; \dots; Z_m) := \sum_{i=1}^m H(Z_i) - H(Z_1, Z_2, \dots, Z_m). \quad (119)$$

Note that $C(Z_1; Z_2; \dots; Z_m)$ can also be written as

$$\sum_{i=2}^m I(Z_i; Z^{i-1}).$$

Suppose \mathbb{R}_+ denotes the set of positive real numbers. Let $k \in \{1, 2, \dots\}$. Consider random variables U_1, U_2, \dots, U_k, V and a set $\mathcal{S} \subseteq [1 : k]$ given by $\mathcal{S} = \{\alpha_1, \alpha_2, \dots, \alpha_{|\mathcal{S}|}\}$. Let $\mathcal{S}^c = [1 : k] \setminus \mathcal{S}$ be denoted by $\mathcal{S}^c = \{\beta_1, \beta_2, \dots, \beta_{k-|\mathcal{S}|}\}$. We define $g_{U_1, U_2, \dots, U_k, V}^{\mathcal{S}} : \mathbb{R}_+^k \rightarrow \mathbb{R}_+$ as

$$\begin{aligned} g_{U_1, U_2, \dots, U_k, V}^{\mathcal{S}}(R_1, R_2, \dots, R_k) &= \left(\sum_{i \in \mathcal{S}} R_i \right) - \\ &\quad C(U_{\alpha_1}; U_{\alpha_2}; \dots; U_{\alpha_{|\mathcal{S}|}}; (U_{\beta_1}, U_{\beta_2}, \dots, U_{\beta_{k-|\mathcal{S}|}}, V)) \end{aligned} \quad (120)$$

Note that the tuple $(U_{\beta_1}, U_{\beta_2}, \dots, U_{\beta_{k-|\mathcal{S}|}}, V)$ is treated as a single random variable. Thus, when $|\mathcal{S}| = 0$,

$$g_{U_1, U_2, \dots, U_k, V}^{\mathcal{S}}(R_1, R_2, \dots, R_k) = 0.$$

Lemma 12: For any $\epsilon > 0$, $n \geq n_0(\epsilon)$, $N_1, N_2, N_3 \geq \exp(n\epsilon)$ and types $P_1 \in \mathcal{P}_{\mathcal{X}_1}^n$, $P_2 \in \mathcal{P}_{\mathcal{X}_2}^n$, $P_3 \in \mathcal{P}_{\mathcal{X}_3}^n$; there exists codebooks $\{\mathbf{x}_{11}, \dots, \mathbf{x}_{1N_1} \in \mathcal{X}_1^n\}$, $\{\mathbf{x}_{21}, \dots, \mathbf{x}_{2N_2} \in \mathcal{X}_2^n\}$, $\{\mathbf{x}_{31}, \dots, \mathbf{x}_{3N_3} \in \mathcal{X}_3^n\}$ whose codewords are of type P_1, P_2, P_3 respectively such that for every permutation (i, j, k) of $(1, 2, 3)$; for every $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$; for every joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}^n$; and for $R_i \stackrel{\text{def}}{=} (1/n) \log_2 N_i$, $R_j \stackrel{\text{def}}{=} (1/n) \log_2 N_j$, and $R_k \stackrel{\text{def}}{=} (1/n) \log_2 N_k$; the statements (121)–(133), shown at the bottom of the next page.

Proof: We will generate the codebooks by a random experiment. For fixed $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$ and joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}^n$, we will show that the probability that each of the statements (121) - (133) does not hold, falls doubly exponentially in n . Since $|\mathcal{X}_i^n|$, $|\mathcal{X}_j^n|$, $|\mathcal{X}_k^n|$ and $|\mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}^n|$ grow only exponentially in n , a union bound will imply that the probability that any of the statements (121) - (133) fail for some $\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k$ and $P_{X_i X'_i X_j X'_j X_k X'_k}$ also falls doubly exponentially. This will show the existence of a codebook satisfying (121) - (133). The proof will

employ Lemma 11 which we have restated below for quick reference.

Lemma 2: For an index set \mathcal{I} , let $\{Y_i : i \in \mathcal{I}\}$ be a set of independent random variables. Let β be a positive integer. Let $\mathcal{J} \subseteq \mathcal{I}^\beta$ be a set of β length tuples consisting of distinct elements from \mathcal{I} . For $(i_1, \dots, i_\beta) \in \mathcal{J}$, let $V_{(i_1, \dots, i_\beta)}$ be a binary random variable which is a function of $Y_{i_1}, \dots, Y_{i_\beta}$. Suppose $U = \sum_{(i_1, \dots, i_\beta) \in \mathcal{J}} V_{(i_1, \dots, i_\beta)}$. For

$$\text{Ex} := \mathbb{E} \left[\sum_{\substack{(j_1, \dots, j_\beta) \in \mathcal{J}: \\ (j_1, \dots, j_\beta) \sim [a, (i_1, \dots, i_\beta)]}} V_{(j_1, \dots, j_\beta)} \right]$$

(i) *Joint typicality of a codeword*

$$|\{r \in [1 : N_i] : (\mathbf{x}_{ir}, \mathbf{x}_k) \in T_{X_i X_k}^n\}| \leq \exp \left\{ n \left(|R_i - I(X_i; X_k)|^+ + \epsilon/2 \right) \right\}; \quad (121)$$

$$|\{s \in [1 : N_j] : (\mathbf{x}_i, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n\}| \leq \exp \left\{ n \left(|R_j - I(X_j; X_i, X_k)|^+ + \epsilon/2 \right) \right\}; \quad (122)$$

$$|\{u \in [1 : N_i] : (\mathbf{x}_{iu}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X_i X_j X_k}^n\}| \leq \exp \left(n \left(|R_1 - I(X'_i; X_i X_j X_k)|^+ + \epsilon/2 \right) \right); \quad (123)$$

(ii) *Joint typicality of a pair of codewords*

$$\begin{aligned} & |\{(r, s) \in [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n\}| \\ & \leq \exp \left\{ n \left(|R_i - I(X_i; X_k)|^+ + |R_j - I(X_j; X_k)|^+ - I(X_i; X_j | X_k) \right)^+ + \epsilon/2 \right\}; \end{aligned} \quad (124)$$

$$\begin{aligned} & |\{(r, u) \in [1 : N_i] \times [1 : N_i] : (\mathbf{x}_{ir}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X'_i X_k}^n, r \neq u\}| \\ & \leq \exp \left\{ n \left(|R_i - I(X_i; X_k)|^+ + |R_i - I(X'_i; X_k)|^+ - I(X_i; X'_i | X_k) \right)^+ + \epsilon/2 \right\}; \end{aligned} \quad (125)$$

$$\begin{aligned} & |\{(s, v) \in [1 : N_j] \times [1 : N_j] : (\mathbf{x}_{js}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_j X'_j X_k}^n, s \neq v\}| \\ & \leq \exp \left\{ n \left(|R_j - I(X_j; X_k)|^+ + |R_j - I(X'_j; X_k)|^+ - I(X_j; X'_j | X_k) \right)^+ + \epsilon/2 \right\}; \end{aligned} \quad (126)$$

$$\begin{aligned} & |\{(r, w) \in [1 : N_i] \times [1 : N_k] : (\mathbf{x}_{ir}, \mathbf{x}_{kw}, \mathbf{x}_k) \in T_{X_i, X'_k, X_k}^n\}| \\ & \leq \exp \left\{ n \left(|R_i - I(X_i; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ - I(X_i; X'_k | X_k) \right)^+ + \epsilon/2 \right\}; \end{aligned} \quad (127)$$

$$\begin{aligned} & |\{(s, w) \in [1 : N_j] \times [1 : N_k] : (\mathbf{x}_{js}, \mathbf{x}_{kw}, \mathbf{x}_k) \in T_{X_j, X'_k, X_k}^n\}| \\ & \leq \exp \left\{ n \left(|R_j - I(X_j; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ - I(X_j; X'_k | X_k) \right)^+ + \epsilon/2 \right\}; \end{aligned} \quad (128)$$

$$\begin{aligned} & |\{(u, v) \in [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp \left(n \left(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_j - I(X'_j; X_i X_j X_k)|^+ - I(X'_i; X'_j | X_i X_j X_k) \right)^+ + \epsilon/2 \right); \end{aligned} \quad (129)$$

$$\begin{aligned} & |\{(u, w) \in [1 : N_i] \times [1 : N_k] : (\mathbf{x}_{iu}, \mathbf{x}_{kw}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp \left(n \left(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_k - I(X'_k; X_i X_j X_k)|^+ - I(X'_i; X'_k | X_i X_j X_k) \right)^+ + \epsilon/2 \right); \end{aligned} \quad (130)$$

(iii) *Joint typicality of three codewords*

$$\begin{aligned} & |\{(r, s, u) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X'_i X_k}^n, r \neq u\}| \\ & \leq \max_{S \subseteq \{1, 2, 3\}} \exp \left\{ n \left(g_{X_i, X_j, X'_i, X_k}^S(R_i, R_j, R_i) + \epsilon/2 \right) \right\}; \end{aligned} \quad (131)$$

(iv) *Joint typicality of four codewords*

$$\begin{aligned} & |\{(r, s, u, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n, r \neq u, s \neq v\}| \\ & \leq \max_{S \subseteq \{1, 2, 3, 4\}} \exp \left\{ n \left(g_{X_i, X_j, X'_i, X'_j, X_k}^S(R_i, R_j, R_i, R_j) + \epsilon/2 \right) \right\}; \text{ and} \end{aligned} \quad (132)$$

$$\begin{aligned} & |\{(r, s, u, w) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_k] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_k X_k}^n, r \neq u\}| \\ & \leq \max_{S \subseteq \{1, 2, 3, 4\}} \exp \left\{ n \left(g_{X_i, X_j, X'_i, X'_k, X_k}^S(R_i, R_j, R_i, R_k) + \epsilon/2 \right) \right\}. \end{aligned} \quad (133)$$

$$\left| (Y_{i_1}, \dots, Y_{i_\beta}) = (y_{i_1}, \dots, y_{i_\beta}) \right|,$$

let

$$E \geq \max \left\{ \left(\max_{(i_1, \dots, i_\beta) \in \mathcal{J}} \max_{\substack{y_{i_1}, \dots, y_{i_\beta}, \\ a \in \mathcal{H}_{(i_1, \dots, i_\beta)} \\ 1 \leq |a| \leq \beta-1}} \mathbb{E} x \right), \mathbb{E}[U] \right\}, \quad (134)$$

For $\gamma > 0$, $\nu > 1$ if there exists $\delta_1, \delta_2, \dots, \delta_\beta > 1$ such that for all $i \in [1 : \beta]$, $\frac{1}{(2\beta)^\beta} \left(\frac{\delta_{i-1}-1}{2\gamma} E - \beta! \right) > \delta_i E$ for $\delta_0 := \nu$, then

$$\mathbb{P}(U \geq \nu E) \leq (|\mathcal{I}| \beta + 1)^{\beta^2} e^{-\gamma/3}. \quad (135)$$

Let $T_l^n, l \in \{1, 2, 3\}$ denote the type class of P_l . We generate independent random codebooks for each user. The codebook for user $l \in \{1, 2, 3\}$, denoted by $(\mathbf{X}_{l1}, \mathbf{X}_{l2}, \dots, \mathbf{X}_{lN_l})$, consists of independent random vectors each distributed uniformly on T_l^n . Fix $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$ and a joint type $P_{X_i X'_i X_j X'_j X_k X'_k} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}^n$ such that for $l \in \{1, 2, 3\}$, $P_{X_l} = P_{X'_l} = P_l$ and $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X_i X_j X_k}^n$.

In order to obtain (121) - (133), we will use $\nu = \exp(n\epsilon/2)$ and $\gamma = \exp(n\epsilon/4\beta)$ in Lemma 11. For $i \in [1 : \beta]$, let $\delta_i = \exp\left(\frac{(4\beta-3i)n\epsilon}{8\beta}\right)$. Note that $\delta_i \geq 1$ for all $i \in [1 : \beta]$, $\delta_0 = \exp(n\epsilon/2) = \nu$ and there exists n_0 s.t. for all $n \geq n_0$,

$$\begin{aligned} \delta_i &= \exp\left(\frac{(4\beta-3i)n\epsilon}{8\beta}\right) \\ &< \left(\exp\left(\frac{(4\beta-3i+1)n\epsilon}{8\beta}\right) \right) \\ &= \frac{\delta_{i-1}}{\gamma} \\ &\approx \frac{1}{(2\beta)^\beta} \left(\frac{\delta_{i-1}-1}{2\gamma} - \frac{\beta!}{E} \right) \text{ for large n.} \end{aligned}$$

The choice of $\beta, \mathcal{I}, \mathcal{J}$ and the random variables will depend on the specific statement among (121) - (133). Though, β will only range in $\{1, 2, 3, 4\}$.

(i) *Analysis of (121), (122) and (123) (Joint typicality of a codeword):* To obtain (121), choose $\mathcal{I} = \{i1, i2, \dots, iN_i\}$ and the set $\{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\}$ corresponding to $\{Y_i : i \in \mathcal{I}\}$. We choose $\beta = 1$ and $\mathcal{J} = \{(i1), (i2), \dots, (iN_i)\}$. For all $r \in [1 : N_i]$,

$$V_{(ir)} = \begin{cases} 1, & \text{if } \mathbf{X}_{ir} \in T_{X_i|X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases}$$

Note that

$$\begin{aligned} \mathbb{P}(V_{(ir)} = 1) &= \frac{|T_{X_i|X_k}^n(\mathbf{x}_k)|}{|T_{X_i}^n|} \\ &\leq \frac{\exp\{nH(X_i|X_k)\}}{(n+1)^{|\mathcal{X}_i|} \exp\{nH(X_i)\}} \\ &= (n+1)^{-|\mathcal{X}_i|} \exp\{-nI(X_i; X_k)\} \\ &\stackrel{(a)}{\leq} \exp\{-nI(X_i; X_k)\} \end{aligned}$$

where (a) follows because $(n+1)^{-|\mathcal{X}_i|} \leq 1$.

Note that $U = \sum_{r \in [1:N_i]} V_{(ir)} = |\{r \in [1:N_i] : (\mathbf{X}_{ir}, \mathbf{x}_k) \in T_{X_i|X_k}^n\}|$. Note that for the case of $\beta = 1$, condition (134) reduces to $E \geq \mathbb{E}[U]$. Thus, $\mathbb{E}[U] = \sum_{r \in [1:N_i]} \mathbb{E}[V_{(ir)}] = \sum_{r \in [1:N_i]} \mathbb{P}(V_{(ir)} = 1) \leq \exp\{n(R_i - I(X_i; X_k))\} \leq \exp\{n|R_i - I(X_i; X_k)|^+\} := E$. Thus, (135) gives us

$$\begin{aligned} \mathbb{P}\left(|\{r \in [1:N_i] : (\mathbf{X}_{ir}, \mathbf{x}_k) \in T_{X_i|X_k}^n\}| \geq \exp\{n(|R_i - I(X_i; X_k)|^+ + \epsilon/2)\}\right) \\ \leq (N_i + 1)e^{-\exp(n\epsilon/4)/3}. \end{aligned} \quad (136)$$

Replacing x_k with (x_i, x_j, x_k) , X_k with (X_i, X_j, X_k) , and X_i with X'_i in the above argument, one can show that

$$\begin{aligned} \mathbb{P}\left(|\{u \in [1:N_i] : (\mathbf{X}_{iu}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i|X_j|X_k}^n\}| \geq \exp\{n(|R_i - I(X'_i; X_j X_k X_k)|^+ + \epsilon/2)\}\right) \\ \leq (N_i + 1)e^{-\exp(n\epsilon/4)/3}. \end{aligned} \quad (137)$$

Similarly, choosing $\mathcal{I} = \{j1, j2, \dots, jN_j\}$, $\{Y_j : j \in \mathcal{I}\} = \{\mathbf{X}_{j1}, \mathbf{X}_{j2}, \dots, \mathbf{X}_{jN_j}\}$, $\mathcal{J} = \{(j1), (j2), \dots, (jN_j)\}$ and replacing \mathbf{x}_k with $(\mathbf{x}_i, \mathbf{x}_k)$, X_k with (X_i, X_k) , and R_j with R_j in the proof of (136), we can show that

$$\begin{aligned} \mathbb{P}\left(|\{s \in [1:N_j] : (\mathbf{x}_i, \mathbf{X}_{js}, \mathbf{x}_k) \in T_{X_i|X_j|X_k}^n\}| \geq \exp\{n(|R_j - I(X_j; X_i X_k)|^+ + \epsilon/2)\}\right) \\ \leq (N_j + 1)e^{-\exp(n\epsilon/4)/3}. \end{aligned} \quad (138)$$

(ii) *Analysis of (124) - (130) (Joint Typicality of a Pair of Codewords):* We will only analyse (124) and (125). The analysis of other statements is similar. To show (124), choose $\mathcal{I} = \{i1, i2, \dots, iN_i\} \cup \{j1, j2, \dots, jN_j\}$, $\{Y_i : i \in \mathcal{I}\} = \{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\} \cup \{\mathbf{X}_{j1}, \mathbf{X}_{j2}, \dots, \mathbf{X}_{jN_j}\}$. For $\beta = 2$, let $\mathcal{J} = \{(ir, js) : (r, s) \in [1:N_i] \times [1:N_j]\}$. For all $(r, s) \in [1:N_i] \times [1:N_j]$,

$$V_{(ir,js)} = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{js}) \in T_{X_i|X_j|X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases}$$

This implies that $U = \sum_{(r,s) \in [1:N_i] \times [1:N_j]} V_{(ir,js)} = |\{(r, s) \in [1:N_i] \times [1:N_j] : (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{x}_k) \in T_{X_i|X_j|X_k}^n\}|$. Note that

$$\begin{aligned} \mathbb{P}(V_{(ir,js)} = 1) &= \frac{|T_{X_i|X_j|X_k}^n(\mathbf{x}_k)|}{|T_{X_i}^n| |T_{X_j}^n|} \\ &\leq \frac{\exp\{nH(X_i X_j|X_k)\}}{(n+1)^{|\mathcal{X}_i|+|\mathcal{X}_j|} \exp\{n(H(X_i) + H(X_j))\}} \\ &= (n+1)^{-(|\mathcal{X}_i|+|\mathcal{X}_j|)} \exp\{-n(H(X_i X_j) - H(X_i X_j|X_k) \\ &\quad - H(X_i X_j) + H(X_i) + H(X_j))\} \\ &= (n+1)^{-(|\mathcal{X}_i|+|\mathcal{X}_j|)} \exp\{-n(I(X_i X_j; X_k) + I(X_i; X_j))\} \\ &\leq \exp\{-n(I(X_i X_j; X_k) + I(X_i; X_j))\} \\ &= \exp\{-n(I(X_j; X_k) + I(X_i; X_k) + I(X_i; X_j))\} \end{aligned}$$

$$= \exp \{-n(I(X_j; X_k) + I(X_i; X_j X_k))\}.$$

Thus,

$$\begin{aligned} \mathbb{E}[U] &= \sum_{(r,s) \in [1:N_i] \times [1:N_j]} \mathbb{E}[V_{(ir,js)}] \\ &= \sum_{(r,s) \in [1:N_i] \times [1:N_j]} \mathbb{P}(V_{(ir,js)} = 1) \\ &\leq \exp \{n(R_i + R_j - I(X_i; X_j X_k) - I(X_j; X_k))\} \\ &\leq \exp \left\{ n \left| R_i - I(X_i; X_k) \right|^+ + \left| R_j - I(X_j; X_k) \right|^+ \right. \\ &\quad \left. - I(X_i; X_j | X_k) \right|^+ \right\} := E. \end{aligned} \quad (139)$$

We need to show that for any $(ir, js) \in \mathcal{J}$, and $(\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js})$,

$$\begin{aligned} E &\geq \max \left(\mathbb{E} \left[\sum_{v \neq s} V_{(ir,jv)} | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}) \right], \right. \\ &\quad \left. \mathbb{E} \left[\sum_{u \neq r} V_{(iu,js)} | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}) \right] \right). \end{aligned}$$

Note that

$$\begin{aligned} &\mathbb{E} \left[\sum_{v \neq s} V_{(ir,jv)} | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}) \right] \\ &= \sum_{v \neq s} \mathbb{E}[V_{(ir,jv)} | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js})] \\ &\leq \sum_{v \neq s} \mathbb{P}(V_{(ir,jv)} = 1 | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js})) \\ &= \sum_{v \neq s} \mathbb{P}(\mathbf{X}_{jv} \in T_{X_j | X_i X_k}^n(\mathbf{x}_{ir}, \mathbf{x}_k)) \\ &= \sum_{v \neq s} \frac{|T_{X_j | X_i X_k}^n(\mathbf{x}_{ir}, \mathbf{x}_k)|}{|T_{X_j}^n|} \\ &\leq \exp\{nR_j\} \frac{\exp\{nH(X_j | X_i X_k)\}}{(n+1)^{|\mathcal{X}_j|} \exp\{nH(X_j)\}} \\ &\leq \exp\{n(|R_j - I(X_j; X_i X_k)|^+)\} \\ &\leq E. \end{aligned} \quad (140)$$

Similarly, we can show that $\mathbb{E} \left[\sum_{u \neq r} V_{(iu,js)} | (\mathbf{X}_{ir}, \mathbf{X}_{js}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}) \right] \leq E$.

Thus, (135) implies that

$$\begin{aligned} &\mathbb{P} \left(\left\{ (r, s) \in [1:N_i] \times [1:N_j] : (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n \right\} \right. \\ &\quad \left. \geq \exp \left\{ n \left(\left| R_i - I(X_i; X_k) \right|^+ + \left| R_j - I(X_j; X_k) \right|^+ \right. \right. \\ &\quad \quad \left. \left. - I(X_i; X_j | X_k) \right|^+ + \epsilon/2 \right) \right\} \\ &\leq ((N_i + N_j)2 + 1)^4 e^{-\exp(n\epsilon/8)/3}. \end{aligned} \quad (141)$$

To show (125), let $\mathcal{I} = \{i1, i2, \dots, iN_i\}$ and $\{Y_i : i \in \mathcal{I}\} = \{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\}$. We choose $\beta = 2$ and

$\mathcal{J} = \{(ir, iu) : (r, u) \in [1:N_i] \times [1:N_i] \text{ such that } r \neq u\}$.
For all (r, u) such that $r \in [1:N_i]$ and $u \in [1:N_i] \setminus \{r\}$,

$$V_{(ir, iu)} = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{iu}) \in T_{X_i X_i' | X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases}$$

By replacing X_j with X'_j in the proof of (141) and following similar arguments, we can show that

$$\begin{aligned} \mathbb{P} \left(\left| \left\{ (r, u) \in [1:N_i] \times [1:N_i] : (\mathbf{x}_{ir}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_i' X_k}^n, \right. \right. \right. \\ \left. \left. \left. r \neq u \right\} \right| \geq \exp \left\{ n \left(\left| R_i - I(X_i; X_k) \right|^+ + \right. \right. \\ \left. \left. \left| R_i - I(X_i'; X_k) \right|^+ - I(X_i; X_i' | X_k) \right|^+ + \epsilon/2 \right) \right\} \right) \\ \leq (2N_i + 1)^4 e^{-\exp(n\epsilon/8)/3}. \end{aligned} \quad (142)$$

(iii) *Analysis of (131) (Joint Typicality of Three Codewords)*
Choose $\mathcal{I} = \{i1, i2, \dots, iN_i\} \cup \{j1, j2, \dots, jN_j\}$, $\{Y_i : i \in \mathcal{I}\} = \{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\} \cup \{\mathbf{X}_{j1}, \mathbf{X}_{j2}, \dots, \mathbf{X}_{jN_j}\}$. For $\beta = 3$, let $\mathcal{J} = \{(ir, js, iu) : (r, s, u) \in [1:N_i] \times [1:N_j] \times [1:N_i], r \neq u\}$. For all $(ir, js, iu) \in \mathcal{J}$,

$$V_{(ir, js, iu)} = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) \in T_{X_i X_j X_i' | X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, $U = \sum_{(ir, js, iu) \in \mathcal{J}} V_{(ir, js, iu)} = |\{(r, s, u) \in [1:N_i] \times [1:N_j] \times [1:N_i] : (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_k}^n, r \neq u\}|$.

Note that

$$\begin{aligned} \mathbb{P}(V_{(ir, js, iu)} = 1) &= \frac{|T_{X_i X_j X_i' | X_k}^n(\mathbf{x}_k)|}{|T_{X_i}^n| |T_{X_j}^n| |T_{X_i'}^n|} \\ &\leq \frac{\exp\{nH(X_i X_j X_i' | X_k)\}}{(n+1)^{2|\mathcal{X}_i| + |\mathcal{X}_j|} \exp\{n(H(X_i) + H(X_j) + H(X_i'))\}} \\ &= (n+1)^{-(2|\mathcal{X}_i| + |\mathcal{X}_j|)} \exp\{n(H(X_i X_j X_i' | X_k) - H(X_i) \\ &\quad - H(X_j) - H(X_i') - H(X_k))\} \\ &\stackrel{(a)}{=} (n+1)^{-(|\mathcal{X}_i| + |\mathcal{X}_j|)} \exp\{-n(C(X_i; X_j; X_i'; X_k))\} \\ &\leq \exp\{-n(C(X_i; X_j; X_i'; X_k))\} \end{aligned}$$

where (a) follows from (119).

Note that

$$\mathbb{E}[U] = \sum_{(ir, js, iu) \in \mathcal{J}} \mathbb{E}[V_{(ir, js, iu)}] \quad (143)$$

$$= \sum_{(ir, js, iu) \in \mathcal{J}} \mathbb{P}(V_{(ir, js, iu)} = 1) \quad (144)$$

$$\leq \exp\{n(2R_i + R_j - C(X_i; X_j; X_i'; X_k))\} \quad (145)$$

$$\leq \max_{S \subseteq \{1, 2, 3\}} \exp\left\{n\left(g_{X_i, X_j, X_i', X_k}^S(R_i, R_j, R_i)\right)\right\}. \quad (146)$$

This is because for $S = \{1, 2, 3\}$, $\exp\{n(g_{X_i, X_j, X_i', X_k}^S(R_i, R_j, R_i))\} = \exp\{n(2R_i + R_j - C(X_i; X_j; X_i'; X_k))\}$. Let $E := \max_{S \subseteq \{1, 2, 3\}} \exp\left\{n\left(g_{X_i, X_j, X_i', X_k}^S(R_i, R_j, R_i)\right)\right\}$.

Using similar arguments as the ones used to obtain (139) and (140), we can show that for any $(ir, js, iu) \in \mathcal{J}$, and $(\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu})$, the lower bound (147) on E , shown at the bottom of the next page.

Thus, we can use (135) to obtain

$$\begin{aligned} \mathbb{P} \left(\left| \{(r, s, u) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] : \right. \right. \\ \left. \left. (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_k}^n, r \neq u\} \right| > \right. \\ \left. \max_{S \subseteq \{1, 2, 3\}} \exp \left\{ n \left(g_{X_i, X_j, X_i', X_k}^S(R_i, R_j, R_i, R_k) + \epsilon/2 \right) \right\} \right) \\ \leq (3(N_i + N_j) + 1)^9 e^{-\exp(n\epsilon/12)/3}. \end{aligned} \quad (148)$$

(iv) *Analysis of (132) and (133) (Joint Typicality of Four Codewords):* We will start with analysis of (133). Choose $\mathcal{I} = \{i1, i2, \dots, iN_i\} \cup \{j1, j2, \dots, jN_j\} \cup \{k1, k2, \dots, kN_k\}$, $\{Y_i : i \in \mathcal{I}\} = \{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\} \cup \{\mathbf{X}_{j1}, \mathbf{X}_{j2}, \dots, \mathbf{X}_{jN_j}\} \cup \{\mathbf{X}_{k1}, \mathbf{X}_{k2}, \dots, \mathbf{X}_{kN_k}\}$. For $\beta = 4$, let $\mathcal{J} = \{(ir, js, iu, kw) : (r, s, u, w) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_k], r \neq u\}$. For all $(ir, js, iu, kw) \in \mathcal{J}$,

$$\begin{aligned} V_{(ir, js, iu, kw)} \\ = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{X}_{kw}) \in T_{X_i X_j X_i' X_k | X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Therefore, $U = \sum_{(ir, js, iu, kw) \in \mathcal{J}} V_{(ir, js, iu, kw)} = |\{(r, s, u, w) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_k] : (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{X}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_k | X_k}^n, r \neq u\}|$.

Note that

$$\begin{aligned} & \mathbb{P}(V_{(ir, js, iu, kw)} = 1) \\ &= \frac{|T_{X_i X_j X_i' X_k | X_k}^n(\mathbf{x}_k)|}{|T_{X_i}^n| |T_{X_j}^n| |T_{X_i'}^n| |T_{X_k}^n|} \\ &\leq \exp \{nH(X_i X_j X_i' X_k | X_k\} \\ &\quad \cdot \frac{(n+1)^{-2|\mathcal{X}_i| - |\mathcal{X}_j| - |\mathcal{X}_k|}}{\exp \{n(H(X_i) + H(X_j) + H(X_i') + H(X_k'))\}} \\ &= (n+1)^{-(2|\mathcal{X}_i| + |\mathcal{X}_j|)} \exp \{n(H(X_i X_j X_i' X_k | X_k) - H(X_i) \\ &\quad - H(X_j) - H(X_i') - H(X_k') - H(X_k))\} \\ &\stackrel{(a)}{=} (n+1)^{-(|\mathcal{X}_i| + |\mathcal{X}_j|)} \exp \{-n(C(X_i; X_j; X_i'; X_k'; X_k))\} \\ &\leq \exp \{-n(C(X_i; X_j; X_i'; X_k'; X_k))\} \end{aligned}$$

where (a) follows from (119).

Note that $\mathbb{E}[U] = \sum_{(ir, js, iu, kw) \in \mathcal{J}} \mathbb{E}[V_{(ir, js, iu, kw)}] = \sum_{(ir, js, iu, kw) \in \mathcal{J}} \mathbb{P}(V_{(ir, js, iu, kw)} = 1) \leq \exp \{n(2R_i + R_j + R_k - C(X_i; X_j; X_i'; X_k'; X_k))\} \leq \max_{S \subseteq \{1, 2, 3, 4\}} \exp \{n(g_{X_i, X_j, X_i', X_k, X_k}^S(R_i, R_j, R_i, R_k))\}$. This is because for $S = \{1, 2, 3, 4\}$, $\exp \{n(g_{X_i, X_j, X_i', X_k, X_k}^S(R_i, R_j, R_i, R_k))\} = \exp \{n(2R_i + R_j + R_k - C(X_i; X_j; X_i'; X_k'; X_k))\}$. Using similar arguments as used on (139), (140) and (146), one can show that $E := \max_{S \subseteq \{1, 2, 3, 4\}} \exp \{n(g_{X_i, X_j, X_i', X_k, X_k}^S(R_i, R_j, R_i, R_k))\}$ satisfies condition (134). Using (135), we obtain

that

$$\begin{aligned} & \mathbb{P} \left(\left| \{(r, s, u, w) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_k] : \right. \right. \\ & \left. \left. (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{X}_{kw}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_k | X_k}^n, r \neq u\} \right| \right. \\ & \left. > \max_{S \subseteq \{1, 2, 3, 4\}} \exp \left\{ n \left(g_{X_i, X_j, X_i', X_k, X_k}^S(R_i, R_j, R_i, R_k) \right. \right. \right. \\ & \left. \left. \left. + \epsilon/2 \right) \right\} \right) \\ & \leq (4(N_i + N_j + N_k) + 1)^{16} e^{-\exp(n\epsilon/16)/3}. \end{aligned} \quad (149)$$

The analysis of (132) is very similar to that of (133). For (132), we choose $\mathcal{I} = \{i1, i2, \dots, iN_i\} \cup \{j1, j2, \dots, jN_j\}$, $\{Y_i : i \in \mathcal{I}\} = \{\mathbf{X}_{i1}, \mathbf{X}_{i2}, \dots, \mathbf{X}_{iN_i}\} \cup \{\mathbf{X}_{j1}, \mathbf{X}_{j2}, \dots, \mathbf{X}_{jN_j}\}$. For $\beta = 4$, let $\mathcal{J} = \{(ir, js, iu, jv) : (r, s, u, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_j], r \neq u, s \neq v\}$. For all $(ir, js, iu, jv) \in \mathcal{J}$,

$$\begin{aligned} V_{(ir, js, iu, jv)} \\ = \begin{cases} 1, & \text{if } (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{X}_{jv}) \in T_{X_i X_j X_i' X_j | X_k}^n(\mathbf{x}_k), \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

We follow the same analysis as done for (133) to obtain

$$\begin{aligned} & \mathbb{P} \left(\left| \{(r, s, u, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_j] : \right. \right. \\ & \left. \left. (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}, \mathbf{X}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_j | X_k}^n, r \neq u, s \neq v\} \right| \right. \\ & \left. > \max_{S \subseteq \{1, 2, 3, 4\}} \exp \left\{ n \left(g_{X_i, X_j, X_i', X_j, X_k}^S(R_i, R_j, R_i, R_j) + \epsilon/2 \right) \right\} \right) \\ & \leq (4(N_i + N_j) + 1)^{16} e^{-\exp(n\epsilon/16)/3}. \end{aligned} \quad (150)$$

□

Lemma 12 gives Lemma 4 as a corollary, which we prove in the next subsection.

C. Codebook

We restate Lemma 4 below and show how it follows from Lemma 12.

Lemma 3: For any $\epsilon > 0$, $n \geq n_0(\epsilon)$, $N_1, N_2, N_3 \geq \exp(n\epsilon)$ and types $P_1 \in \mathcal{P}_{\mathcal{X}_1}^n$, $P_2 \in \mathcal{P}_{\mathcal{X}_2}^n$, $P_3 \in \mathcal{P}_{\mathcal{X}_3}^n$, there exists codebooks $\{\mathbf{x}_{11}, \dots, \mathbf{x}_{1N_1} \in \mathcal{X}_1^n\}$, $\{\mathbf{x}_{21}, \dots, \mathbf{x}_{2N_2} \in \mathcal{X}_2^n\}$, $\{\mathbf{x}_{31}, \dots, \mathbf{x}_{3N_3} \in \mathcal{X}_3^n\}$ whose codewords are of type P_1, P_2, P_3 respectively such that for every permutation (i, j, k) of $(1, 2, 3)$; for every $(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in \mathcal{X}_i^n \times \mathcal{X}_j^n \times \mathcal{X}_k^n$; for every joint type $P_{X_i X_j X_i' X_j X_k X_k'} \in \mathcal{P}_{\mathcal{X}_i \times \mathcal{X}_i \times \mathcal{X}_j \times \mathcal{X}_j \times \mathcal{X}_k \times \mathcal{X}_k}$; and for $R_i \stackrel{\text{def}}{=} (1/n) \log_2 N_i$, $R_j \stackrel{\text{def}}{=} (1/n) \log_2 N_j$, and $R_k \stackrel{\text{def}}{=} (1/n) \log_2 N_k$; the statements (151)–(157), shown at the bottom of the next page.

Proof: We will use the following identity, which follows from the chain rule of mutual information, throughout the proof. For random variables U, V and W , the following holds,

$$\begin{aligned} I(U; W) + I(V; W) + I(U; V|W) &= I(U; VW) \\ + I(V; W) &= I(U; W) + I(V; UW). \end{aligned} \quad (158)$$

Below we use this identity without an explicit mention. Statements (151)–(153) are statements (123), (129) and (130),

restated directly from Lemma 12. To show (154), we divide the LHS and RHS of (124) by $N_i N_j$ and substitute the expression for the notation given by (120) to obtain

$$\begin{aligned} & \frac{|\{(r, s) \in [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n\}|}{N_i N_j} \\ & < \exp \left\{ n \left(\left| |R_i - I(X_i; X_k)|^+ + |R_j - I(X_j; X_k)|^+ \right. \right. \right. \\ & \quad \left. \left. \left. - I(X_i; X_j | X_k) \right|^+ + \epsilon/2 - R_i - R_j \right) \right\}. \end{aligned}$$

We will evaluate the RHS for different values of R_i and R_j . We see that when $R_i \leq I(X_i; X_k)$, the RHS is

$$\begin{aligned} & \exp \left\{ n \left(|R_j - I(X_j; X_i X_k)|^+ - R_j + \epsilon/2 - R_i \right) \right\} \\ & \leq \exp \{ n(\epsilon/2 - R_i) \} \\ & \stackrel{(a)}{\leq} \exp \{ -n\epsilon/2 \}, \end{aligned}$$

$$\begin{aligned} E & \geq \max \left(\mathbb{E} \left[\sum_{v \neq s} V_{(ir, jv, iu)} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right], \mathbb{E} \left[\sum_{r' \notin \{r, u\}} V_{(ir', js, iu)} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right], \right. \\ & \mathbb{E} \left[\sum_{u' \notin \{r, u\}} V_{(ir, js, iu')} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right], \mathbb{E} \left[\sum_{r', u' \notin \{r, u\}} V_{(ir', js, iu')} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right], \\ & \left. \mathbb{E} \left[\sum_{r' \notin \{r, u\}, v \neq s} V_{(ir', jv, iu)} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right], \mathbb{E} \left[\sum_{u' \notin \{r, u\}, v \neq s} V_{(ir, jv, iv)} \middle| (\mathbf{X}_{ir}, \mathbf{X}_{js}, \mathbf{X}_{iu}) = (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}) \right] \right). \end{aligned} \quad (147)$$

$$|\{u \in [1 : N_i] : (\mathbf{x}_{iu}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X_j X_k}^n\}| \leq \exp \left(n \left(|R_1 - I(X'_1; X_1 X_2 X_3)|^+ + \epsilon/2 \right) \right); \quad (151)$$

$$\begin{aligned} & |\{(u, v) \in [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp \left(n \left(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_j - I(X'_j; X_i X_j X_k)|^+ - I(X'_i; X'_j | X_i X_j X_k)|^+ + \epsilon/2 \right) \right); \end{aligned} \quad (152)$$

$$\begin{aligned} & |\{(u, w) \in [1 : N_i] \times [1 : N_k] : (\mathbf{x}_{iu}, \mathbf{x}_{kw}, \mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \in T_{X'_i X'_j X_i X_j X_k}^n\}| \\ & \leq \exp \left(n \left(|R_i - I(X'_i; X_i X_j X_k)|^+ + |R_k - I(X'_k; X_i X_j X_k)|^+ - I(X'_i; X'_k | X_i X_j X_k)|^+ + \epsilon/2 \right) \right); \end{aligned} \quad (153)$$

$$\frac{1}{N_i N_j} |\{(r, s) \in [1 : N_i] \times [1 : N_j] : (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n\}| < \exp \left(-\frac{n\epsilon}{2} \right), \quad \text{if } I(X_i; X_k) + I(X_j; X_i X_k) \geq \epsilon; \quad (154)$$

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1 : N_i] \times [1 : N_j] : \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n\}| \\ & < \exp \left(-\frac{n\epsilon}{2} \right), \end{aligned}$$

$$\text{if } I(X_i; X_j X'_i X'_j X_k) + I(X_j; X'_i X'_j X_k) \geq |R_i - I(X'_i; X_k)|^+ + |R_j - I(X'_j; X_k)|^+ - I(X'_i; X'_j | X_k)|^+ + \epsilon; \quad (155)$$

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1 : N_i] \times [1 : N_j] : \exists (u, w) \in [1 : N_i] \times [1 : N_k], u \neq r, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{kw}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_k X_k}^n\}| \\ & < \exp \left(-\frac{n\epsilon}{2} \right), \end{aligned}$$

$$\text{if } I(X_i; X_j X'_i X'_k X_k) + I(X_j; X'_i X'_k X_k) \geq |R_i - I(X'_i; X_k)|^+ + |R_k - I(X'_k; X_k)|^+ - I(X'_i; X'_k | X_k)|^+ + \epsilon; \quad (156)$$

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1 : N_i] \times [1 : N_j] : \exists u \in [1 : N_i], u \neq r, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X'_i X_k}^n\}| < \exp \left(-\frac{n\epsilon}{2} \right), \\ & \text{if } I(X_i; X_j X'_i X_k) + I(X_j; X'_i X_k) \geq |R_i - I(X'_i; X_k)|^+ + \epsilon. \end{aligned} \quad (157)$$

where (a) holds because $R_i > \epsilon$. Similarly, we can show the same upper bound of $\exp \{n(-\epsilon/2)\}$ when $R_j \leq I(X_j; X_k)$. When $R_i + R_j \leq I(X_i; X_k) + I(X_j; X_k) + I(X_i; X_j | X_k)$, the RHS is upper bounded by $\exp(n(\epsilon/2 - R_i - R_j)) \leq \exp(-n\epsilon/2)$. When $R_i > I(X_i; X_k)$, $R_j > I(X_j; X_k)$ and $R_i + R_j > I(X_i; X_k) + I(X_j; X_k) + I(X_i; X_j | X_k)$, the RHS evaluates to (using (158))

$$\begin{aligned} & \exp \{n(-I(X_i; X_k) - I(X_j; X_i X_k) + \epsilon/2)\} \\ & \leq \exp \{-n\epsilon/2\}, \quad \text{if } I(X_i; X_k) + I(X_j; X_i X_k) \geq \epsilon. \end{aligned}$$

Next, we will prove (157). For this, we will first show that

$$\begin{aligned} & \frac{1}{N_i N_j} |\{(r, s) \in [1 : N_i] \times [1 : N_j] : \exists u \in [1 : N_i], u \neq r, \\ & (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X'_i X_k}^n\}| < \exp \left(-\frac{n\epsilon}{2} \right), \end{aligned} \quad (159)$$

if any one of the following hold:

$$R_i + R_j - \max_{\mathcal{S} \subseteq \{1,2,3\}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i) \geq \epsilon, \quad (160)$$

$$\begin{aligned} R_i + R_j - & \left| |R_i - I(X_i; X_k)|^+ + |R_j - I(X_j; X_k)|^+ \right. \\ & \left. - I(X_i; X_j | X_k) \right|^+ \geq \epsilon. \end{aligned} \quad (161)$$

We now show that (160) implies (159):

$$\begin{aligned} & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \exists u \in [1 : N_i], u \neq r, \right. \right. \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X'_i X_k}^n \right\} \right| \\ & \stackrel{(a)}{\leq} \exp \left(-n \left(R_i + R_j - \max_{\mathcal{S} \subseteq \{1,2,3\}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i) - \epsilon/2 \right) \right) \\ & \leq \exp \left(-\frac{n\epsilon}{2} \right) \end{aligned}$$

if $R_i + R_j - \max_{\mathcal{S} \subseteq \{1,2,3\}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i) \geq \epsilon$, where (a) follows from (131). Next, we show that (161) implies (159).

$$\begin{aligned} & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \exists u \in [1 : N_i], u \neq r, \right. \right. \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X_j X'_i X_k}^n \right\} \right| \\ & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n \right\} \right| \\ & \stackrel{(a)}{\leq} \exp \left(-n \left(R_i + R_j - \left| |R_i - I(X_i; X_k)|^+ \right. \right. \right. \\ & \quad \left. \left. \left. + |R_j - I(X_j; X_k)|^+ - I(X_i; X_j | X_k) \right|^+ - \epsilon/2 \right) \right) \\ & \leq \exp \left(-\frac{n\epsilon}{2} \right) \end{aligned}$$

$$\begin{aligned} & \text{if } R_i + R_j - \left| |R_i - I(X_i; X_k)|^+ + |R_j - I(X_j; X_k)|^+ \right. \\ & \quad \left. - I(X_i; X_j | X_k) \right|^+ \geq \epsilon, \end{aligned}$$

where (a) follows from (124). Now, we will show that the condition in (157) implies at least one of (160) or (161). We restate the condition in (157) below for quick reference.

$$I(X_i; X_j X'_i X_k) + I(X_j; X'_i X_k) \geq |R_i - I(X'_i; X_k)|^+ + \epsilon \quad (162)$$

To show that (162) implies at least one of (160) or (161), we will do case analysis based on the value of $\hat{\mathcal{S}} \stackrel{\text{def}}{=} \arg\max_{\mathcal{S}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i)$, the set of maximizers of the expression $g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i)$ in (160). Evaluations of $g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j)$ under different values of $\hat{\mathcal{S}}$ are provided in Table I. The table also gives the implications when $\tilde{\mathcal{S}} \in \arg\max_{\mathcal{S}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i)$ in the fourth column. For example, the (6) row considers the case of $\{1,3\} \in \arg\max_{\mathcal{S}} g_{X_i, X_j, X'_i, X_k}^{\mathcal{S}}(R_i, R_j, R_i)$. Under this case, we have, for instance, $g_{X_i, X_j, X'_i, X_k}^{\{1,3\}}(R_i, R_j, R_i) \geq g_{X_i, X_j, X'_i, X_k}^{\{1,2,3\}}(R_i, R_j, R_i)$, i.e., $R_i - I(X_i; X_j X_k) + R_i - I(X'_i; X_i X_j X_k) \geq R_j - I(X_j; X_k) + R_i - I(X_i; X_j X_k) \geq R_j - I(X_j; X_k) + R_i - I(X_i; X_j X_k)$.

$I(X'_i; X_i X_j X_k)$. Hence, $R_j \leq I(X_j; X_k)$. This implication is given in the fifth column of the table against the “reason” (6) \geq (8) where (8) is the row corresponding to $\mathcal{S} = \{1,2,3\}$. The other implications are also easy to see from the table. Instead of providing all the implications, the table only provide the ones which we will use in the proof of (157).

Case 1 ($\tilde{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\tilde{\mathcal{S}}| \leq 1$): In this case, (160) holds as $R_i, R_j \geq \epsilon$.

Case 2 ($\tilde{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\tilde{\mathcal{S}}| = 2$): If $\{1,2\} \in \hat{\mathcal{S}}$, then it can be seen from the expression of $g_{X_i, X_j, X'_i, X_k}^{\{1,2\}}(R_i, R_j, R_i)$ from Table I that (162) implies (160). If $\{1,3\} \in \hat{\mathcal{S}}$, then $R_j \leq I(X_j; X_k)$. This implies that the LHS of (161) evaluates to

$$R_i + R_j - |R_i - I(X_i; X_j X_k)|^+$$

which is at least ϵ because $R_j \geq \epsilon$. Thus, (161) holds. Similarly, when $\{2,3\} \in \hat{\mathcal{S}}$, one can use the fact that $R_i \leq I(X_i; X_k)$ and $R_i \geq \epsilon$ to show that (161) holds.

Case 3 ($\tilde{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\tilde{\mathcal{S}}| = 3$): In this case, $R_i \geq I(X'_i; X_k)$. Thus, conditions (162) and (160) are same. Thus, (162) implies (160).

Now, we will now show (155). Its proof is very similar to the proof of (157). To show (155), we will first show that

$$\begin{aligned} & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\ & \quad \left. \left. \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \right. \right. \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right| < \exp \left(-\frac{n\epsilon}{2} \right) \end{aligned} \quad (163)$$

if any one of the following inequalities hold:

$$R_i + R_j - \max_{\mathcal{S} \subseteq \{1,2,3,4\}} g_{X_i, X_j, X'_i, X'_j, X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j) \geq \epsilon, \quad (164)$$

$$\begin{aligned} R_j - & \left| |R_j - I(X_j; X_k)|^+ + |R_i - I(X'_i; X_k)|^+ \right. \\ & \left. - I(X_j; X'_j | X_k) \right|^+ \geq \epsilon, \end{aligned} \quad (165)$$

$$\begin{aligned} R_j - & \left| |R_j - I(X_j; X_k)|^+ + |R_j - I(X'_j; X_k)|^+ \right. \\ & \left. - I(X_j; X'_j | X_k) \right|^+ \geq \epsilon, \end{aligned} \quad (166)$$

$$\begin{aligned} R_i - & \left| |R_i - I(X_i; X_k)|^+ + |R_i - I(X'_i; X_k)|^+ \right. \\ & \left. - I(X_i; X'_i | X_k) \right|^+ \geq \epsilon, \end{aligned} \quad (167)$$

$$\begin{aligned} R_i - & \left| |R_i - I(X_i; X_k)|^+ + |R_j - I(X'_j; X_k)|^+ \right. \\ & \left. - I(X_i; X'_j | X_k) \right|^+ \geq \epsilon, \end{aligned} \quad (168)$$

$$\begin{aligned} R_i + R_j - & \left| |R_i - I(X_i; X_k)|^+ + |R_j - I(X_j; X_k)|^+ \right. \\ & \left. - I(X_i; X_j | X_k) \right|^+ \geq \epsilon. \end{aligned} \quad (169)$$

The fact that (164) implies (163) can be shown as follows:

$$\begin{aligned} & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] \exists (u, v) \in [1 : N_i] \times [1 : N_j], \right. \right. \\ & \quad \left. \left. u \neq r, v \neq s, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right| \end{aligned}$$

TABLE I
TABLE SHOWING DIFFERENT EVALUATIONS OF $\max_{S \subseteq \{1,2,3\}} g_{X_i, X_j, X'_i, X_k}^S(R_i, R_j, R_i)$ AND THEIR IMPLICATIONS

Index	\tilde{S}	$g_{X_i, X_j, X'_i, X_k}^{\tilde{S}}(R_i, R_j, R_i)$	Implications of $\tilde{S} \in \arg\max_S g_{X_i, X_j, X'_i, X_k}^S(R_i, R_j, R_i)$	reasons
(1)	\emptyset	0		
(2)	{1}	$R_i - I(X_i; X_j X'_i X_k)$		
(3)	{2}	$R_j - I(X_j; X_i X'_i X_k)$		
(4)	{3}	$R_i - I(X'_i; X_i X_j X_k)$		
(5)	{1, 2}	$R_i - I(X_i; X'_i X_k) + R_j - I(X_j; X_i X'_i X_k)$		
(6)	{1, 3}	$R_i - I(X_i; X_j X_k) + R_i - I(X'_i; X_i X_j X_k)$	$R_j \leq I(X_j; X_k)$	(6) \geq (8)
(7)	{2, 3}	$R_j - I(X_j; X_i X_k) + R_i - I(X'_i; X_i X_j X_k)$	$R_i \leq I(X_i; X_k)$	(7) \geq (8)
(8)	{1, 2, 3}	$R_i - I(X_i; X_k) + R_j - I(X_j; X_i X_k) + R_i - I(X'_i; X_i X_j X_k)$	$R_i \geq I(X'_i; X_k)$	(8) \geq (5)

$$\begin{aligned}
 & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s, u, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. u \neq r, v \neq s, (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right| \\
 & \stackrel{(a)}{\leq} \exp \left(-n \left(R_i + R_j - \max_{S \in \{1, 2, 3, 4\}} g_{X_i, X_j, X'_i, X'_j, X_k}^S(R_i, R_j, R_i, R_j) - \epsilon/2 \right) \right) \\
 & \leq \exp(-n\epsilon/2) \\
 & \text{if } R_i + R_j - g_{X_i, X_j, X'_i, X'_j, X_k}^S(R_i, R_j, R_i, R_j) \geq \epsilon, \text{ where (a) uses (132). Next we show that (165) implies (163).}
 \end{aligned}$$

$$\begin{aligned}
 & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \right. \right. \\
 & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right|
 \end{aligned}$$

$$\begin{aligned}
 & \leq \frac{1}{N_i N_j} \left| \left\{ \left| (r, s, u) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] : \right. \right. \right. \\
 & \quad \left. \left. \left. (\mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_j X'_i X_k}^n \right\} \right| \\
 & = \frac{1}{N_i N_j} \left| \left\{ \left| \left\{ r \in [1 : N_i] \right\} \times \left\{ (s, u) \in [1 : N_j] \times [1 : N_i] : \right. \right. \right. \right. \\
 & \quad \left. \left. \left. \left. (\mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_j X'_i X_k}^n \right\} \right\} \right| \\
 & = \frac{1}{N_j} \left| \left\{ \left| \left\{ (s, u) \in [1 : N_j] \times [1 : N_i] : \right. \right. \right. \right. \\
 & \quad \left. \left. \left. \left. (\mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_j X'_i X_k}^n \right\} \right\} \right|
 \end{aligned}$$

$$\begin{aligned}
 & \stackrel{(a)}{\leq} \exp \left(-n \left(R_j - \left| |R_j - I(X_j; X_k)|^+ + |R_i - I(X'_i; X_k)|^+ - I(X_j; X'_i | X_k) |^+ - \epsilon/2 \right| \right) \right)
 \end{aligned}$$

$$\leq \exp(-n\epsilon/2)$$

$$\begin{aligned}
 & \text{if } R_j - \left| |R_j - I(X_j; X_k)|^+ + |R_i - I(X'_i; X_k)|^+ - I(X_j; X'_i | X_k) |^+ \geq \epsilon,
 \end{aligned}$$

where (a) uses (125) with X_i replaced with X'_i . The remaining conditions can also be obtained similarly. We can show that (166) implies (163) by using (126) on the following upper bound.

$$\frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right.$$

$$\begin{aligned}
 & \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \\
 & \quad (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \Big\} \Big| \\
 & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. s \neq v, (\mathbf{x}_{js}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_j X'_j X_k}^n \right\} \right| \\
 & = \frac{1}{N_j} \left| \left\{ (s, v) \in [1 : N_j] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. s \neq v, (\mathbf{x}_{js}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_j X'_j X_k}^n \right\} \right|.
 \end{aligned}$$

To show that (167) implies (163), we use the following upper bound and (125).

$$\begin{aligned}
 & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \right. \right. \\
 & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right| \\
 & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s, u) \in [1 : N_i] \times [1 : N_j] \times [1 : N_i] : \right. \right. \\
 & \quad \left. \left. r \neq u, (\mathbf{x}_{ir}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X'_i X_k}^n \right\} \right| \\
 & = \frac{1}{N_i} \left| \left\{ (r, u) \in [1 : N_i] \times [1 : N_i] : \right. \right. \\
 & \quad \left. \left. r \neq u, (\mathbf{x}_{ir}, \mathbf{x}_{iu}, \mathbf{x}_k) \in T_{X_i X'_i X_k}^n \right\} \right|.
 \end{aligned}$$

The condition (168) can be obtained similarly by using (125) (with X_j replaced with X'_j) on the following upper bound:

$$\begin{aligned}
 & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \right. \right. \\
 & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X'_i X'_j X_k}^n \right\} \right| \\
 & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s, v) \in [1 : N_i] \times [1 : N_j] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X'_j X_k}^n \right\} \right| \\
 & = \frac{1}{N_i} \left| \left\{ (r, v) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\
 & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X'_j X_k}^n \right\} \right|.
 \end{aligned}$$

For (169), we use (124) on the following upper bound:

$$\begin{aligned} & \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\ & \quad \exists (u, v) \in [1 : N_i] \times [1 : N_j], u \neq r, v \neq s, \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_{iu}, \mathbf{x}_{jv}, \mathbf{x}_k) \in T_{X_i X_j X_i' X_j' X_k}^n \right\} \right| \\ & \leq \frac{1}{N_i N_j} \left| \left\{ (r, s) \in [1 : N_i] \times [1 : N_j] : \right. \right. \\ & \quad \left. \left. (\mathbf{x}_{ir}, \mathbf{x}_{js}, \mathbf{x}_k) \in T_{X_i X_j X_k}^n \right\} \right|. \end{aligned}$$

Now to show (155), we will show that the condition in (155) implies at least one of (164)-(168). We restate the condition in (155) below for quick reference.

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq \left| R_i - I(X_i'; X_k) \right| + \left| R_j - I(X_j'; X_k) \right| \\ & \quad - I(X_i'; X_j' | X_k) \left| + \epsilon. \right. \quad (170) \end{aligned}$$

To show that (170) implies at least one of (164)-(168), we do a case analysis similar to the one in proof of (157). The case analysis will be based on the value of $\hat{\mathcal{S}} \stackrel{\text{def}}{=} \arg\max_{\mathcal{S}} g_{X_i, X_j, X_i', X_j', X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j)$, the set of maximizers of the expression $g_{X_i, X_j, X_i', X_j', X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j)$ in (164). For ease of reference, evaluations of the expression $g_{X_i, X_j, X_i', X_j', X_k}^{\hat{\mathcal{S}}}(R_i, R_j, R_i, R_j)$ under different values of $\hat{\mathcal{S}}$ are given in Table II. Table II is similar to Table I. It also gives the implications when $\hat{\mathcal{S}} \in \arg\max_{\mathcal{S} \subseteq \{1, 2, 3, 4\}} g_{X_i, X_j, X_i', X_j', X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j)$ in the fourth column. For example, the ⑨-th row considers the case of $\{2, 3\} \in \arg\max_{\mathcal{S}} g_{X_i, X_j, X_i', X_j', X_k}^{\mathcal{S}}(R_i, R_j, R_i, R_j)$. Under this case, $g_{X_i, X_j, X_i', X_j', X_k}^{\{2, 3\}}(R_i, R_j, R_i, R_j) \geq g_{X_i, X_j, X_i', X_j', X_k}^{\{1, 2, 3\}}(R_i, R_j, R_i, R_j)$, i.e., $R_j - I(X_j; X_i X_j' X_k) + R_i - I(X_i'; X_i X_j' X_k) \geq R_i - I(X_i; X_i' X_k) + R_j - I(X_j; X_i X_j' X_k) + R_i - I(X_i'; X_i X_j X_j' | X_k)$. This implies that $R_i \leq I(X_i; X_i' X_k)$. It is given in the fifth column of the table against the “reason” ⑨ \geq ⑯ where ⑯ is the row corresponding to $\mathcal{S} = \{1, 2, 3\}$. The other implications can also be seen easily from the table.

Case 1 ($\hat{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\hat{\mathcal{S}}| \leq 1$): For this case, substituting the expression of $g_{X_i, X_j, X_i', X_j', X_k}^{\hat{\mathcal{S}}}(R_i, R_j, R_i, R_j)$ from Table II and noting $R_i, R_j \geq \epsilon$, we see that (164) holds.

Case 2 ($\hat{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\hat{\mathcal{S}}| = 2$): We start with $\{1, 2\} \in \hat{\mathcal{S}}$. For this case, (164) evaluates to $I(X_i; X_i' X_j' X_k) + I(X_i; X_i' X_j' X_j X_k) \geq \epsilon$ which is directly implied by (170). If $\{1, 3\} \in \hat{\mathcal{S}}$, we see from Table II that $R_j \leq I(X_j; X_j' X_k)$, $R_j \leq I(X_j'; X_j X_k)$ and $R_j - I(X_j; X_k) + R_j - I(X_j'; X_k) - I(X_j; X_j' | X_k) \leq 0$. This implies that $\left| R_j - I(X_j; X_k) \right| + \left| R_j - I(X_j'; X_k) \right| - I(X_j; X_j' | X_k) = 0$. Thus, by noting that $R_j \geq \epsilon$, (166) holds. Similarly; if $\{1, 4\} \in \hat{\mathcal{S}}$, (165) holds; if $\{2, 3\} \in \hat{\mathcal{S}}$, (168) holds; if $\{2, 4\} \in \hat{\mathcal{S}}$, (167) holds; and if $\{3, 4\} \in \hat{\mathcal{S}}$, (169) holds.

Case 3 ($\hat{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\hat{\mathcal{S}}| = 3$): If $\{2, 3, 4\} \in \hat{\mathcal{S}}$, from Table II, $R_i \leq I(X_i; X_k)$. This implies that the LHS

of (169) is $R_i + R_j - |R_j - I(X_j; X_i X_k)|^+$ which is at least ϵ because $R_i \geq \epsilon$. Thus, (169) holds. Similarly, for $\{1, 3, 4\} \in \hat{\mathcal{S}}$, $R_j \leq I(X_j; X_k)$, which implies that (169) holds. If $\{1, 2, 4\} \in \hat{\mathcal{S}}$, from Table II, $R_i \leq I(X_i'; X_k)$ and $R_j \geq I(X_j'; X_i X_k)$. These imply that (170) evaluates to

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq R_j - I(X_j'; X_i' X_k) + \epsilon. \end{aligned}$$

Moreover, since $\{1, 2, 4\} \in \hat{\mathcal{S}}$, (164) evaluates to

$$\begin{aligned} & R_i + R_j - \left(R_i - I(X_i; X_j' X_k) + R_j - I(X_j; X_i X_j' X_k) \right. \\ & \quad \left. + R_j - I(X_j'; X_i X_j X_i' X_k) \right) \geq \epsilon. \end{aligned}$$

It can be seen upon rearranging that (170) and (164) are the same. Thus, (170) implies (164). Similarly, for $\mathcal{S} = \{1, 2, 3\}$, (170) evaluates to

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq R_i - I(X_i'; X_j' X_k) + \epsilon, \end{aligned}$$

which implies (164).

For $\mathcal{S} = \{1, 2, 3\}$, $R_j \leq I(X_j'; X_k)$ and $R_i \geq I(X_i'; X_j' X_k)$. This implies that (170) evaluates to

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq R_i - I(X_i'; X_j' X_k) + \epsilon. \end{aligned}$$

and for $\mathcal{S} = \{1, 2, 3\}$, (164) evaluates to

$$\begin{aligned} & R_i + R_j - \left(R_i - I(X_i; X_j' X_k) + R_j - I(X_j; X_i X_j' X_k) \right. \\ & \quad \left. + R_i - I(X_i'; X_i X_j X_j' X_k) \right) \geq \epsilon. \end{aligned}$$

It can be seen upon rearranging that the above two inequalities are the same. Thus, (170) implies (164) if $\{1, 2, 4\} \in \hat{\mathcal{S}}$. Similarly, for $\mathcal{S} = \{1, 2, 4\}$, (170) evaluates to

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq R_j - I(X_j'; X_i' X_k) + \epsilon, \end{aligned}$$

which implies (164).

Case 4 ($\hat{\mathcal{S}} \in \hat{\mathcal{S}}$ Such That $|\hat{\mathcal{S}}| = 4$): For $\{1, 2, 3, 4\} \in \hat{\mathcal{S}}$, (170) evaluates to

$$\begin{aligned} & I(X_i; X_j X_i' X_j' X_k) + I(X_j; X_i' X_j' X_k) \\ & \geq R_j - I(X_j'; X_k) + R_i - I(X_i'; X_j' X_k) + \epsilon, \end{aligned}$$

and (164) evaluates to

$$\begin{aligned} & R_i + R_j - 2R_i - 2R_j + I(X_j'; X_k) + I(X_i'; X_j' X_k) \\ & \quad + I(X_j; X_i' X_j' X_k) + I(X_i; X_j X_i' X_j' X_k) \geq \epsilon, \end{aligned}$$

which is same as (170). Thus, (170) implies (164).

Statement (156) can be proved similarly by using (124), (125), (127), (128) and (133), the equivalent statements of (124)-(126) and (132) on replacing \mathbf{x}_{jv} , X_j' and the corresponding rate R_j with \mathbf{x}_{kw} , X_k' and the corresponding rate R_k respectively. In fact, by making these replacements in the proof of (155), we obtain the proof of (156). Note that the proof of (155) only depended on (124)-(126) and (132). \square

TABLE II
TABLE SHOWING DIFFERENT EVALUATIONS OF $\max_{S \subseteq \{1, 2, 3, 4\}} g_{X_i, X_j, X'_i, X'_j, X_k}^S(R_i, R_j, R_i, R_j)$ AND THEIR IMPLICATIONS

Index	$\tilde{\mathcal{S}}$	$g_{X_i, X_j, X'_i, X'_j, X_k}^{\tilde{\mathcal{S}}}(R_i, R_j, R_i, R_j)$	Implications of $\tilde{\mathcal{S}} \in \arg\max_{S \subseteq \{1, 2, 3, 4\}} g_{X_i, X_j, X'_i, X'_j, X_k}^S(R_i, R_j, R_i, R_j)$	reasons
①	\emptyset	0		
②	{1}	$R_i - I(X_i; X_j X'_i X'_j X_k)$		
③	{2}	$R_j - I(X_j; X_i X'_i X'_j X_k)$		
④	{3}	$R_i - I(X'_i; X_i X_j X'_j X_k)$		
⑤	{4}	$R_j - I(X'_j; X_i X_j X'_i X_k)$		
⑥	{1, 2}	$R_i - I(X_i; X'_i X'_j X_k) + R_j - I(X_j; X_i X'_i X'_j X_k)$		
⑦	{1, 3}	$R_i - I(X_i; X_j X'_j X_k) + R_i - I(X'_i; X_i X_j X'_j X_k)$	$R_j \leq I(X_j; X'_j X_k)$ $R_j \leq I(X'_j; X_j X_k)$ $R_j - I(X_j; X_k) + R_j - I(X'_j; X_j X_k) \leq 0$	$(7) \geq (15)$ $(7) \geq (13)$ $(7) \geq (16)$
⑧	{1, 4}	$R_i - I(X_i; X_j X'_i X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_j \leq I(X_j; X'_i X_k)$ $R_i \leq I(X'_i; X_j X_k)$ $R_j - I(X_j; X_k) + R_i - I(X'_i; X_j X_k) \leq 0$	$(8) \geq (14)$ $(8) \geq (13)$ $(8) \geq (16)$
⑨	{2, 3}	$R_j - I(X_j; X_i X'_j X_k) + R_i - I(X'_i; X_i X_j X'_j X_k)$	$R_i \leq I(X_i; X'_j X_k)$ $R_j \leq I(X'_j; X_i X_k)$ $R_i - I(X_i; X_k) + R_j - I(X'_j; X_i X_k) \leq 0$	$(9) \geq (15)$ $(9) \geq (12)$ $(9) \geq (16)$
⑩	{2, 4}	$R_j - I(X_j; X_i X'_i X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_i \leq I(X_i; X'_i X_k)$ $R_i \leq I(X'_i; X_i X_k)$ $R_i - I(X_i; X_k) + R_j - I(X'_i; X_i X_k) \leq 0$	$(10) \geq (14)$ $(10) \geq (12)$ $(10) \geq (16)$
⑪	{3, 4}	$R_i - I(X'_i; X_i X_j X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_i \leq I(X_i; X_j X_k)$ $R_j \leq I(X_j; X_i X_k)$ $R_i - I(X_i; X_k) + R_j - I(X_j; X_i X_k) \leq 0$	$(11) \geq (13)$ $(11) \geq (12)$ $(11) \geq (16)$
⑫	{2, 3, 4}	$R_j - I(X_j; X_i X_k) + R_i - I(X'_i; X_i X_j X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_i \leq I(X_i; X_k)$	$(12) \geq (16)$
⑬	{1, 3, 4}	$R_i - I(X_i; X_j X_k) + R_i - I(X'_i; X_i X_j X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_j \leq I(X_j; X_k)$	$(13) \geq (16)$
⑭	{1, 2, 4}	$R_i - I(X_i; X'_i X_k) + R_j - I(X_j; X_i X'_i X_k) + R_j - I(X'_j; X_i X_j X'_i X_k)$	$R_i \leq I(X'_i; X_k)$ $R_j \geq I(X'_j; X_i X_k)$	$(14) \geq (16)$ $(14) \geq (6)$
⑮	{1, 2, 3}	$R_i - I(X_i; X'_j X_k) + R_j - I(X_j; X_i X'_j X_k) + R_i - I(X'_i; X_i X_j X'_j X_k)$	$R_j \leq I(X_j; X_k)$ $R_i \geq I(X'_i; X'_j X_k)$	$(15) \geq (16)$ $(15) \geq (6)$
⑯	{1, 2, 3, 4}	$R_i - I(X_i; X_k) + R_j - I(X_j; X_i X_k) + R_i - I(X'_i; X_i X_j X_k) + R_j - I(X'_j; X'_i X_i X_j X_k)$	$R_i > I(X'_i; X_k)$ $R_j \geq I(X'_j; X_k)$ $R_i - I(X'_i; X_k) + R_j - I(X'_j; X'_i X_i X_j X_k) \geq 0$	$(16) \geq (14)$ $(16) \geq (15)$ $(16) \geq (6)$

APPENDIX III PROOF OF LEMMA 6

This appendix gives the proof of Lemma 6. We restate it here for completeness.

Lemma 4: For any $\mathcal{Q}_1, \dots, \mathcal{Q}_t \in \mathcal{A}$, $t \in \mathbb{N}$ and $\mathcal{Q} \subseteq [1 : k]$ such that $\mathcal{Q} = \bigcap_{i=1}^t \mathcal{Q}_i$, $P_{e, \mathcal{Q}} \leq \sum_{i=1}^t P_{e, \mathcal{Q}_i}$.

Proof of Lemma 6:

$$\begin{aligned}
 P_{e, \mathcal{Q}} &= \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{(\prod_{j \in \mathcal{Q}} N_j)} \sum_{m_{\mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}}} \mathbb{P}(\{\phi(\mathbf{Y})_{\mathcal{Q}} \neq m_{\mathcal{Q}}\} | \mathbf{X}_{\mathcal{Q}} = f_{\mathcal{Q}}(m_{\mathcal{Q}}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \\
 &= \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{(\prod_{j \in \mathcal{Q}} N_j)} \sum_{m_{\mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}}} \mathbb{P}(\bigcup_{i=1}^t \{\phi(\mathbf{Y})_{\mathcal{Q}_i} \neq m_{\mathcal{Q}_i}\} | \mathbf{X}_{\mathcal{Q}} = f_{\mathcal{Q}}(m_{\mathcal{Q}}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \\
 &\stackrel{(a)}{\leq} \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{(\prod_{j \in \mathcal{Q}} N_j)} \sum_{m_{\mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}}} \sum_{i=1}^t \mathbb{P}(\{\phi(\mathbf{Y})_{\mathcal{Q}_i} \neq m_{\mathcal{Q}_i}\} | \mathbf{X}_{\mathcal{Q}} = f_{\mathcal{Q}}(m_{\mathcal{Q}}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \\
 &= \sum_{i=1}^t \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{(\prod_{j \in \mathcal{Q}} N_j)} \sum_{m_{\mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}}} \mathbb{P}(\{\phi(\mathbf{Y})_{\mathcal{Q}_i} \neq m_{\mathcal{Q}_i}\} | \mathbf{X}_{\mathcal{Q}} = f_{\mathcal{Q}}(m_{\mathcal{Q}}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}})
 \end{aligned}$$

$$\begin{aligned}
 &\stackrel{(b)}{\leq} \sum_{i=1}^t \max_{\mathbf{x}_{\mathcal{Q}_i}} \frac{1}{(\prod_{j \in \mathcal{Q}_i} N_j)} \sum_{m_{\mathcal{Q}_i} \in \mathcal{M}_{\mathcal{Q}_i}} \mathbb{P}(\{\phi(\mathbf{Y})_{\mathcal{Q}_i} \neq m_{\mathcal{Q}_i}\} | \mathbf{X}_{\mathcal{Q}_i} = f_{\mathcal{Q}_i}(m_{\mathcal{Q}_i}), \mathbf{X}_{\mathcal{Q}_i} = \mathbf{x}_{\mathcal{Q}_i}) \\
 &= \sum_{i=1}^t \max_{\mathbf{x}_{\mathcal{Q}_i}} \frac{1}{(\prod_{j \in \mathcal{Q}_i} N_j)} \sum_{m_{\mathcal{Q}_i} \in \mathcal{M}_{\mathcal{Q}_i}} \mathbb{P}(\{\phi(\mathbf{Y})_{\mathcal{Q}_i} \neq m_{\mathcal{Q}_i}\} | \mathbf{X}_{\mathcal{Q}_i} = f_{\mathcal{Q}_i}(m_{\mathcal{Q}_i}), \mathbf{X}_{\mathcal{Q}_i} = \mathbf{x}_{\mathcal{Q}_i}) \\
 &= \sum_{i=1}^t P_{e, \mathcal{Q}_i},
 \end{aligned}$$

where (a) follows from a union bound. To see (b) note that $\mathcal{Q} \subseteq \mathcal{Q}_i$ for any $i \in [1 : t]$ and thus, the maximization is over a larger set. \square

APPENDIX IV PROOF OF ACHIEVABILITY OF THEOREM 7

For the achievability, we will require the following theorem which gives the randomized coding capacity region of a t -user AV-MAC $W_{Y|X_1, \dots, X_t, S}$ where \mathcal{X}_i , $i \in [1 : k]$ are the input alphabets and \mathcal{Y} and \mathcal{S} are the output and the state alphabets respectively. The theorem can be proved along the lines of the two user result given in [8] and [30] (see [8, Remark II A3]).

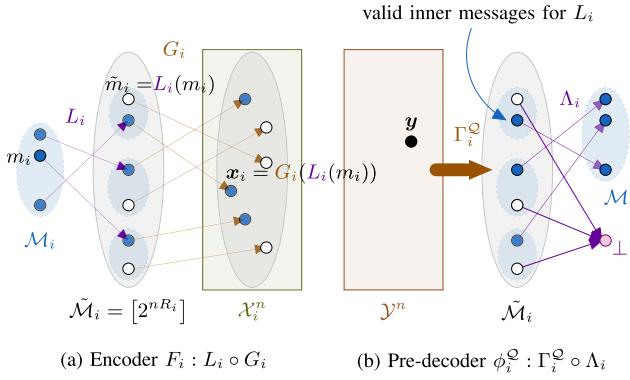


Fig. 16. The encoders and pre-decoders for Theorem 7.

Theorem 13 (AV-MAC Randomized Capacity Region for t -Users): The randomized capacity region of the AV-MAC $W_{Y|X_1, \dots, X_t, S}$ is the set of rate tuples such that

$$\sum_{j \in \mathcal{J}} R_j \leq \min_{q(s|u)} I(X_{\mathcal{J}}; Y|X_{\mathcal{J}^c}, S, U) \text{ for every } \mathcal{J} \subseteq [1 : t] \quad (171)$$

for some joint distribution $p(u)q(s|u) \prod_{i=1}^t p(x_i|u)$ with $|\mathcal{U}| \leq t$.

Proof (Achievability of Theorem 7): This proof is along the lines of the proof of Theorem 3. For each $\mathcal{Q} \in \mathcal{A}$, let $W^{\mathcal{Q}}$ be the $|\mathcal{Q}^c|$ -user AV-MAC which corresponds to users in the set \mathcal{Q} as adversary and the users in the set \mathcal{Q}^c as the legitimate users. For users in \mathcal{Q} , their combined input $x_{\mathcal{Q}}$ and the product input alphabet $\times_{i \in \mathcal{Q}} \mathcal{X}_i$ correspond to the adversarial state input and the state alphabet respectively. Let (R_1, R_2, \dots, R_k) be a rate tuple such that for some $p(u) \cdot p(x_1|u) \cdot p(x_2|u) \dots p(x_k|u)$, the following conditions hold for all $\mathcal{Q} \in \mathcal{A}$ and $\mathcal{J} \subseteq \mathcal{Q}^c$,

$$\sum_{j \in \mathcal{J}} R_j \leq \min_{q(x_{\mathcal{Q}}|u)} I(X_{\mathcal{J}}; Y|X_{(\mathcal{Q} \cup \mathcal{J})^c}, U) \quad (172)$$

where the mutual information above is evaluated using the joint distribution $p(u)q(x_{\mathcal{Q}}|u) \prod_{j \in \mathcal{J}} p(x_j|u)W(y|x_{\mathcal{Q}}, x_{\mathcal{Q}^c})$. Here $|\mathcal{U}| \leq k$. Let $\epsilon > 0$ be arbitrary and let n be large enough. Note that, by Theorem 13, the rate tuple $R_{\mathcal{Q}^c}$ is an achievable rate pair for the AVMAC $W^{\mathcal{Q}}$. For each $i \in [1 : k]$, let $\tilde{\mathcal{M}}_i = [1 : 2^{nR_i}]$ and $\mathcal{M}_i = [1 : 2^{nR_i}/v]$ for the largest integer $v \leq (k|\mathcal{A}|)/\epsilon$. In the following, we show the existence of a randomized $(2^{nR_1}/v, \dots, 2^{nR_k}/v, n)$ code (F_1, \dots, F_k, ϕ) with P_e^{rand} no larger than ϵ , for sufficiently large n .

A. Code Design

Before describing the code, we describe the following maps which will help in describing the encoders and the decoder (see Figure 16). For each user i , let $G_i : \tilde{\mathcal{M}}_i \rightarrow \mathcal{X}_i^n$ be a randomized map such that it maps $m_i \in \tilde{\mathcal{M}}_i$ to an n -length i.i.d. sequence $G_i(m_i)$ generated according to the distribution p_i . The sequences $G_i(m)$ are independent across $i \in [1 : k]$ and $m \in \tilde{\mathcal{M}}_i$. The realization of $G_i(m_i)$ for all $i \in [1 : k]$ and $m_i \in \mathcal{M}_i$ is shared with the decoder. For any $\mathcal{Q} \in \mathcal{A}$, consider the $|\mathcal{Q}^c|$ -user AV-MAC $W^{\mathcal{Q}}$ as described above. For

each $i \in \mathcal{Q}^c$, if we consider $\tilde{\mathcal{M}}_i$ as the message set and G_i as the corresponding encoder, then this construction ensures that the random encoders $G_i, i \in \mathcal{Q}^c$ are independent and their randomness is also private from the adversarial users in the set \mathcal{Q} . Thus, the joint distribution of the encoders $G_i, i \in \mathcal{Q}^c$ (and the corresponding codewords) is the same as that of the encoders of AV-MAC $W^{\mathcal{Q}}$ in the direct part of [8, Theorem 1, Section III-C] (and its extension to a t -user AV-MAC as in Theorem 13). For $G_i, i \in \mathcal{Q}^c$ as encoders, let $\Gamma^{\mathcal{Q}}$ denote the corresponding decoder for the AV-MAC $W^{\mathcal{Q}}$ in Theorem 13. Suppose $(\Gamma_j^{\mathcal{Q}}, j \in \mathcal{Q}^c) := \Gamma^{\mathcal{Q}}$ where $\Gamma_j^{\mathcal{Q}} : \mathcal{Y}^n \rightarrow \tilde{\mathcal{M}}_i$. For all $\epsilon > 0$, by Theorem 13, there exists a large enough n such that for all $\mathcal{Q} \in \mathcal{A}$, the code $((G_i, i \in \mathcal{Q}^c), \Gamma^{\mathcal{Q}})$ has error probability no larger than $\epsilon/(k|\mathcal{A}|)$. We consider that n .

For each $i \in [1 : k]$, the message set \mathcal{M}_i is randomly embedded into the set $\tilde{\mathcal{M}}_i$ as follows: We choose an arbitrary partition of $\tilde{\mathcal{M}}_i$ into $|\mathcal{M}_i|$ many disjoint equal-sized subsets (each subset size is v). Let us denote the partition by \mathcal{S}_{m_i} , $m_i \in \mathcal{M}_i$ where $\cup_{m_i \in \mathcal{M}_i} \mathcal{S}_{m_i} = \tilde{\mathcal{M}}_i$ and $\mathcal{S}_{m_i} \cap \mathcal{S}_{m'_i} = \emptyset$ for all $m_i \neq m'_i$, $m_i, m'_i \in \mathcal{M}_i$. The size of each \mathcal{S}_{m_i} , $m_i \in \mathcal{M}_i$ is v ($\leq (k|\mathcal{A}|)/\epsilon$). The maps $L_i : \mathcal{M}_i \rightarrow \tilde{\mathcal{M}}_i$ and $\Lambda_i : \tilde{\mathcal{M}}_i \rightarrow \mathcal{M}_i$ are the forward and reverse maps for an injection from \mathcal{M}_i to $\tilde{\mathcal{M}}_i$ where, independently for each $m_i \in \mathcal{M}_i$, $L_i(m_i)$ is chosen uniformly at random from \mathcal{S}_{m_i} . Both the encoder maps G_i and L_i are independent for $i = 1, 2, \dots, k$ and are made available to the decoder as the shared secret between user- i and the decoder, unknown to other users.

For the code of the byzantine-MAC, for each $i \in [1 : k]$, the encoder map $F_i : \mathcal{M}_i \rightarrow \mathcal{X}_i^n$ is defined as $F_i(m_i) = G_i(L_i(m_i))$ for every $m_i \in \mathcal{M}_i$. For each $\mathcal{Q} \in \mathcal{A}$ and $i \in \mathcal{Q}^c$, we define pre-decoder¹⁵

$$\phi_i^{\mathcal{Q}}(\mathbf{y}) = \begin{cases} \Lambda_i(\Gamma_i^{\mathcal{Q}}(\mathbf{y})) & \text{if } \Gamma_i^{\mathcal{Q}}(\mathbf{y}) \in L_i(\mathcal{M}_i), \\ \perp & \text{otherwise.} \end{cases}$$

The decoder $\phi : \mathcal{Y}^n \rightarrow \times_{i \in [1:k]} \mathcal{M}_i$ outputs $\phi(\mathbf{y}) = (\hat{m}_1, \dots, \hat{m}_k)$, where, for each $i \in [1 : k]$ and $\mathcal{Q} \in \mathcal{A}$,

$$\begin{aligned} \hat{m}_i &= \begin{cases} \phi_i^{\mathcal{Q}}(\mathbf{y}) & \text{if } |\{\phi_i^{\tilde{\mathcal{Q}}}(\mathbf{y}) : \tilde{\mathcal{Q}} \in \mathcal{A}\}| = 1 \text{ and } \phi_i^{\mathcal{Q}}(\mathbf{y}) \neq \perp \\ \phi_i^{\mathcal{Q}}(\mathbf{y}) & \text{if } \{\phi_i^{\tilde{\mathcal{Q}}}(\mathbf{y}) : \tilde{\mathcal{Q}} \in \mathcal{A}\} = \{\Phi_i^{\mathcal{Q}}(\mathbf{y}), \perp\} \\ & \quad \text{where } \phi_i^{\mathcal{Q}}(\mathbf{y}) \neq \perp \\ 1 & \text{otherwise.} \end{cases} \end{aligned}$$

B. Error Analysis

We first show that as long as the rate tuple (R_1, R_2, \dots, R_k) satisfy the rate constraints (172), the following hold simultaneously for every honest user i which sends message $m_i \in \mathcal{M}_i$, potentially adversarial set of users $\mathcal{Q} \in \mathcal{A}$ with $i \notin \mathcal{Q}$ and for channel output \mathbf{Y} : (i) $\phi_i^{\mathcal{Q}}(\mathbf{Y})$ equals m_i with probability at least $1 - \epsilon/(k|\mathcal{A}|)$ if users \mathcal{Q} are indeed adversarial and (ii) $\phi_i^{\mathcal{Q}}(\mathbf{Y})$ either equals \perp or m_i , with probability at least $1 - \epsilon/(k|\mathcal{A}|)$, if users \mathcal{Q} are not adversarial. To this end, consider $\mathcal{Q} \in \mathcal{A}$ and assume that the adversarial users (if

¹⁵In this notation $\phi_i^{\mathcal{Q}}(\mathbf{y})$, we are suppressing the dependence of the pre-decoder (and later the decoder) on the randomness of the encoders.

any) are users in set \mathcal{Q} which send $\mathbf{X}_{\mathcal{Q}}$ as their potentially adversarial input to the channel. Suppose, for $i \in \mathcal{Q}^c$ and $m_i \in \mathcal{M}_i$, user- i sends $F_i(m_i)$. Let \mathbf{Y} denote the channel output.

(i) First, consider the AV-MAC $W^{\mathcal{Q}}$. Recall that $\Gamma_i^{\mathcal{Q}}(\mathbf{Y}) = L_i(m_i)$ with probability at least $1 - \epsilon/(k|\mathcal{A}|)$. Thus, with probability at least $1 - \epsilon/(k|\mathcal{A}|)$, $\phi_i^{\mathcal{Q}}(\mathbf{Y})$ equals m_i . This also holds for any $\tilde{\mathcal{Q}} \subset \mathcal{Q}$, as we can think of this as adversarial users \mathcal{Q} where users in $\mathcal{Q} \setminus \tilde{\mathcal{Q}}$ send valid codewords.

(ii) Next, consider the AV-MAC $W^{\tilde{\mathcal{Q}}}$, for $\tilde{\mathcal{Q}} \in \mathcal{A}$ where $\tilde{\mathcal{Q}} \setminus \mathcal{Q} \neq \emptyset$. We would like to compute $\mathbb{P}(\phi_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) \notin \{m_i, \perp\})$ where for $i \in \mathcal{Q}^c$, the probability is over $G_i(L_i(m_i))$, $\mathbf{X}_{\mathcal{Q}}$ and the channel.

$$\begin{aligned} & \mathbb{P}(\phi_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) \notin \{m_i, \perp\}) \\ &= \mathbb{P}(\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) = \tilde{m}_i, \tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) = \tilde{m}_i) \\ & \quad \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\}) | \Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) = \tilde{m}_i) \\ &\stackrel{(a)}{=} \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) = \tilde{m}_i) \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &\stackrel{(b)}{=} \sum_{\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}} \mathbb{P}(\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) = \tilde{m}_i) \cdot \frac{1}{v} \\ &\leq 1/v \leq \epsilon/(k|\mathcal{A}|). \end{aligned}$$

Here, (a) holds as $\Gamma_i^{\tilde{\mathcal{Q}}}(\mathbf{Y}) \perp\!\!\!\perp L_i(\mathcal{M}_i \setminus \{m_i\})$. This is because $G_i(L_i(m_i))$ which produces \mathbf{Y} is independent of $L_i(\mathcal{M}_i \setminus \{m_i\})$ and $\Gamma_i^{\tilde{\mathcal{Q}}} \perp\!\!\!\perp L_i(\mathcal{M}_i \setminus \{m_i\})$ as $\Gamma_i^{\tilde{\mathcal{Q}}}$ is a function of AV-MAC encoders $G_i, i \in \tilde{\mathcal{Q}}^c$ which are independent of L_i . The equality (b) holds because for $\tilde{m}_i \in \tilde{\mathcal{M}} \setminus \mathcal{S}_{m_i}$,

$$\begin{aligned} & \mathbb{P}(\tilde{m}_i \in L_i(\mathcal{M}_i \setminus \{m_i\})) \\ &= \sum_{m'_i \in \mathcal{M}_i \setminus \{m_i\}} \mathbb{P}(L_i(m'_i) = \tilde{m}_i) \\ &= \sum_{m'_i \in \mathcal{M}_i \setminus \{m_i\}} 1_{\{\tilde{m}_i \in \mathcal{S}_{m'_i}\}} \cdot \frac{1}{v} \\ &= 1/v. \end{aligned}$$

By taking union bound over all users and all $\mathcal{Q} \in \mathcal{A}$, with probability $1 - \epsilon$, for each non-adversarial user i , at least one of the decoders $\phi_i^{\mathcal{Q}}$, $\mathcal{Q} \in \mathcal{A}$ outputs the true message while the other decoder outputs either the true message or \perp .

□

APPENDIX V RANDOMNESS REDUCTION LEMMA

Lemma 14 (Randomness Reduction): Suppose $\epsilon > 0$. For large enough n , given any (N_1, \dots, N_k, n) randomized code

$(F_{[1:k]}, \phi(F_{[1:k]}))$ satisfying

$$P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi) < 2^{\epsilon/2} - 1,$$

there exist n^2 deterministic encoding maps $f_{j,i}, i \in [1 : n^2]$ for each user $j \in [1 : k]$ such that for every $\mathcal{Q} \in \mathcal{A}, j_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|}$, $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$ and the decoder ϕ ,

$$\begin{aligned} & \frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1 : n^2]^{|\mathcal{Q}^c|}} \frac{1}{(\prod_{i \in \mathcal{Q}^c} N_i)} \\ & \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}\left\{(\phi(\mathbf{Y}, f_{\mathcal{Q}, j_{\mathcal{Q}}}, f_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}) = \hat{m}_{[1:k]} \text{ such that} \right. \\ & \left. \hat{m}_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}) | \mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}\right\} < \epsilon. \end{aligned}$$

Here, $f_{\mathcal{Q}, j_{\mathcal{Q}}}$ denotes $(f_{i, j_i} : i \in \mathcal{Q})$.

Remark 4: Lemma 14 states that given a randomized code with a small probability of error $(2^{\epsilon/2} - 1)$, there exists another randomized code of the same rate for all users which uses only $2 \log n$ random bits at each user such that the new code also has a small probability of error (ϵ).

Proof: The proof follows along the lines of Jahn [8, Theorem 1], though there are significant differences because of the byzantine nature of users. In particular, our result needs to incorporate the fact that a malicious user can maliciously choose their encoding map to influence decoding. For each $i \in [1 : K]$, let $\{F_{ij}\}_{j=1}^{n^2}$ be independent samples of codebook F_i (also independent across i). This gives the set of codes $\{(F_{ij}, \phi(F_{ij})), i \in [1 : K], j \in [1 : n^2], \phi := \phi\}$. For every $\mathcal{Q} \in \mathcal{A}$, define $e_{\mathcal{Q}}(f_{\mathcal{Q}}, f_{\mathcal{Q}^c}, \mathbf{x}_{\mathcal{Q}})$ to be the error probability for fixed encoding maps $f_{\mathcal{Q}}$ for the adversarial users and $f_{\mathcal{Q}^c}$ for the non-adversarial users and the channel inputs chosen by the adversarial users as $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$, i.e.,

$$e_{\mathcal{Q}}(f_{\mathcal{Q}}, f_{\mathcal{Q}^c}, \mathbf{x}_{\mathcal{Q}}) := \frac{1}{(\prod_{i \in \mathcal{Q}^c} N_i)} \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \sum_{\substack{\mathbf{y}: \phi(\mathbf{y}, f_{\mathcal{Q}}, f_{\mathcal{Q}^c}) = \hat{m}_{[1:k]}, \\ \text{where } \hat{m}_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}}} W_{Y|\mathbf{X}_{\mathcal{Q}^c}, \mathbf{X}_{\mathcal{Q}}}(\mathbf{y} | f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}).$$

Note that for $j_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|}$, $j_{\mathcal{Q}^c} \in [1 : n^2]^{|\mathcal{Q}^c|}$, $e_{\mathcal{Q}}(F_{\mathcal{Q}, j_{\mathcal{Q}}}, F_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}})$, as a function of $F_{\mathcal{Q}, j_{\mathcal{Q}}}$ and $F_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}$ is a random variable. We wish to show that

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1 : n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q}, j_{\mathcal{Q}}}, F_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right. \\ \left. \text{for some } \mathcal{Q} \in \mathcal{A}, j_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|} \text{ and } \mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n\right) = 0$$

Using a union bound over $\mathcal{Q} \in \mathcal{A}$, $j_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|}$, and $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$, we have

$$\begin{aligned} & \mathbb{P}\left(\frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1 : n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q}, j_{\mathcal{Q}}}, F_{\mathcal{Q}^c, j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right. \\ & \left. \text{for some } \mathcal{Q} \in \mathcal{A}, j_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|} \text{ and } \mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n\right) \end{aligned}$$

$$\leq \sum_{\substack{\mathcal{Q} \in \mathcal{A}, \\ j_{\mathcal{Q}} \in [1:n^2]^{|\mathcal{Q}|}, \\ \mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n}} \mathbb{P} \left(\frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right)$$

Note that the summands in $\sum_{j_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}})$ are not necessarily independent. Hence, an exponential concentration inequality cannot be directly argued. However, using a similar procedure as Jahn [8, Theorem 1], we decompose this sum into parts that consist of summands that are conditionally independent given the adversary's choices.

To this end, let $\Sigma_{n^2} := \{\tau_i : i \in [0 : n^2 - 1]\}$ be a set of permutations of $\{1, 2, \dots, n^2\}$ with

$$\tau_i(j) = (i + j) \bmod n^2 \text{ for all } j \in [1 : n^2].$$

Suppose $|\mathcal{Q}| = l$ for some $l \in [1 : k]$. For ease of notation, let $Q = \{1, 2, \dots, l\}$. Then,

$$\begin{aligned} & \frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \\ &= \frac{1}{(n^2)^{k-l}} \sum_{(j_{l+1}, \dots, j_k) \in [1:n^2]^{k-l}} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \\ &= \frac{1}{(n^2)^{k-l-1}} \sum_{(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}} \left(\frac{1}{n^2} \sum_{j \in [n^2]} \right. \\ & \quad \left. e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}}) \right). \end{aligned}$$

Now, we have (173)–(175), shown at the top of the next page. We note that $e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}})$ is identically distributed for all $(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}$. Thus, we have (176)–(188), shown at the bottom of the next page, where (a) follows from Markov's inequality. (b), (c) and (d) hold because for each $j \in [1 : n^2]$, conditioned on $F_{\mathcal{Q},j_{\mathcal{Q}}}$, $e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}})$ are i.i.d. random variables taking values between 0 and 1 (recall that $2^t \leq 1 + t$ for $t \in [0 : 1]$). The inequality (e) follows from the definition of $P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi)$ by noting that for every realization $f_{\mathcal{Q}} \in \mathcal{F}_{\mathcal{Q}}$ of $F_{\mathcal{Q},j_{\mathcal{Q}}}$, $\mathbb{E}[e_{\mathcal{Q}}(f_{\mathcal{Q}}, (F_{l+1,1}, F_{l+2,1}, \dots, F_{k,1}), \mathbf{x}_{\mathcal{Q}})] \leq P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi)$. This implies that the random variable

$$\mathbb{E} \left[e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,1}, F_{l+2,1}, \dots, F_{k,1}), \mathbf{x}_{\mathcal{Q}}) \middle| F_{\mathcal{Q},j_{\mathcal{Q}}} \right] \text{ is}$$

upper bounded by $P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi)$. Thus,

$$\begin{aligned} & \mathbb{P} \left(\frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{j_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right. \\ & \quad \left. \text{for some } \mathcal{Q} \in \mathcal{A}, j_{\mathcal{Q}} \in [1:n^2]^{|\mathcal{Q}|} \text{ and } \mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n \right) \\ & \stackrel{(a)}{\leq} 2^k (n^2)^k \prod_{i \in [1:k]} |\mathcal{X}_i|^n \exp \left\{ -n^2 \left(\epsilon \right. \right. \\ & \quad \left. \left. - \log(1 + P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi)) \right) - \frac{k-l-1}{n^2} \log(n^2) \right\} \\ & \rightarrow 0 \text{ for enough } n, \end{aligned}$$

where (a) follows by recalling that $P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi) < 2^{\epsilon/2} - 1$ and thus, $\epsilon > 2 \log(1 + P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi))$. \square

APPENDIX VI PROOF OF LEMMA 10

Proof of Lemma 10: This can be shown along the lines of the proof of [28, Theorem 12.11]. For $\epsilon > 0$ and large enough n , let $(F_{[1:k]}, \phi(F_{[1:k]}))$ be an (N_1, \dots, N_k, n) randomized code satisfying

$$P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi) < 2^{\epsilon/2} - 1.$$

Applying Lemma 14 on this code, for each user $j \in [1 : k]$, we obtain n^2 deterministic encoding maps $f_{j,i}, i \in [1 : n^2]$ such that for every $\mathcal{Q} \in \mathcal{A}, l_{\mathcal{Q}} \in [1 : n^2]^{|\mathcal{Q}|}, \mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$ and the decoder ϕ ,

$$\begin{aligned} & \frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{l_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} \frac{1}{(\prod_{i \in \mathcal{Q}^c} N_i)} \\ & \quad \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P} \left(\left\{ \phi(\mathbf{Y}, f_{\mathcal{Q},l_{\mathcal{Q}}}, f_{\mathcal{Q}^c,l_{\mathcal{Q}^c}}) = \hat{m}_{[1:k]} \text{ such that} \right. \right. \\ & \quad \left. \left. \hat{m}_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c} \right\} \middle| \mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c,l_{\mathcal{Q}^c}}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}} \right) < \epsilon. \end{aligned} \quad (189)$$

Further, since $R_i > 0$ is achievable for all $i \in [1 : k]$, there exists an (n^2, \dots, n^2, k_n) code $(\hat{f}_{[1:k]}, \hat{\phi})$ where $k_n/n \rightarrow 0$ and

$$\max_{\mathcal{Q} \in \mathcal{A}} P_{e,\mathcal{Q}}^{\text{rand}}(\hat{f}_{[1:k]}, \hat{\phi}) \leq \epsilon \quad (190)$$

for large enough n . We choose sufficiently large n such that both (189) and (190) hold. For a vector sequence $\tilde{\mathbf{s}} \in \mathcal{S}^{n+k_n}$ for any alphabet \mathcal{S} , we write $\tilde{\mathbf{s}} = (\hat{\mathbf{s}}, \mathbf{s})$, where $\hat{\mathbf{s}}$ denotes the first k_n -length part of $\tilde{\mathbf{s}}$ and \mathbf{s} denotes the last n -length part of the $\tilde{\mathbf{s}}$. Let $(\hat{f}_{[1:k]}, \hat{\phi})$ be a new $(\tilde{N}_1, \dots, \tilde{N}_k, \tilde{n})$ code where $\tilde{n} := k_n + n$, message set for user- i , $\tilde{\mathcal{M}}_i = [1 : \tilde{N}_i] := \{1, 2, \dots, n^2\} \times [1 : N_i]$. Further, for $l \in [1 : n^2], m \in [1 : N_i]$, let $\tilde{m} := (l, m)$. We define $\tilde{f}_i(\tilde{m}) = \hat{f}_i(l, m) := (\hat{f}_i(l), f_{i,l}(m))$. For $\tilde{\mathbf{y}} = (\hat{\mathbf{y}}, \mathbf{y})$, let $\phi(\tilde{\mathbf{y}}) := (\hat{f}_{[1:k]}, \phi(\mathbf{y}, f_{[1:k],\hat{f}_{[1:k]}}))$ where $\hat{f}_{[1:k]} = \hat{\phi}(\hat{\mathbf{y}})$. Then, for $\mathcal{Q} \in \mathcal{A}$, we have (191), shown at the bottom of the page 2358, where (a) follows from (189) and (190). This completes the proof of the lemma. \square

APPENDIX VII PROOF OF LEMMA 9

We first give the codebook which is given by Lemma 15 below. Its proof is along the lines of [10, Lemma 2] and [22, Lemma 3] and is given later.

Lemma 15: For any $\epsilon > 0$, large enough $n, N \geq \exp(n\epsilon)$ and types $P_i \in \mathcal{P}_{\mathcal{X}_i}^n : i \in [1 : k]$, there exist codebooks $\mathcal{C}_i, i \in [1 : k]$ for message sets $\mathcal{M}_i = [1 : N], i \in [1 : k]$, whose codewords are of type $P_i, i \in [1 : k]$ respectively such that for every $\mathcal{Q} \in \mathcal{A}$ such that $|\mathcal{Q}| < k$,¹⁶ $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n, \mathcal{T} \subseteq \mathcal{Q}^c, \mathcal{J} \subseteq \mathcal{Q}$, and joint type $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{J}}} \in \mathcal{P}_{\mathcal{X}_{\mathcal{Q}^c} \times \mathcal{X}_{\mathcal{Q}} \times \mathcal{X}'_{\mathcal{T}} \times \mathcal{X}'_{\mathcal{J}}}^n$, the following holds:

¹⁶Note that there are no decoding guarantees when all users are malicious, so we only consider the case when at least one user is honest.

$$\begin{aligned} & \mathbb{P} \left(\frac{1}{(n^2)|\mathcal{Q}^c|} \sum_{j_{\mathcal{Q}^c} \in [1:n^2] \setminus \mathcal{Q}^c} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, F_{\mathcal{Q}^c,j_{\mathcal{Q}^c}}, \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right) \\ &= \mathbb{P} \left(\sum_{(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}} \left(\frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}}) \right) \geq (n^2)^{k-l-1} \epsilon \right) \end{aligned} \quad (173)$$

$$\leq \mathbb{P} \left(\bigcup_{(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}} \left\{ \frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right\} \right) \quad (174)$$

$$\leq \sum_{(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}} \mathbb{P} \left\{ \frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right\}. \quad (175)$$

$$\begin{aligned} & \sum_{(\sigma_{l+2}, \sigma_{l+3}, \dots, \sigma_k) \in \Sigma_{n^2}^{k-l-1}} \mathbb{P} \left\{ \frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\sigma_{l+2}(j)}, \dots, F_{k,\sigma_k(j)}), \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right\} \\ & \leq (n^2)^{k-l-1} \mathbb{P} \left\{ \frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,\tau_0(j)}, \dots, F_{k,\tau_0(j)}), \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right\} \end{aligned} \quad (176)$$

$$= (n^2)^{k-l-1} \mathbb{P} \left\{ \frac{1}{n^2} \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}}) \geq \epsilon \right\} \quad (177)$$

$$= (n^2)^{k-l-1} \mathbb{P} \left\{ \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}}) \geq n^2 \epsilon \right\} \quad (178)$$

$$= (n^2)^{k-l-1} \mathbb{P} \left\{ \exp \left\{ \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}}) \right\} \geq \exp \{n^2 \epsilon\} \right\} \quad (179)$$

$$\stackrel{(a)}{\leq} (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E} \left[\exp \left\{ \sum_{j \in [n^2]} e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}}) \right\} \right] \quad (180)$$

$$= (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E} \left[\prod_{j \in [n^2]} \exp \{e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}})\} \right] \quad (181)$$

$$= (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E}_{F_{\mathcal{Q},j_{\mathcal{Q}}}} \left[\mathbb{E} \left[\prod_{j \in [n^2]} \exp \{e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}})\} \middle| F_{\mathcal{Q},j_{\mathcal{Q}}} \right] \right] \quad (182)$$

$$\stackrel{(b)}{=} (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E}_{F_{\mathcal{Q},j_{\mathcal{Q}}}} \left[\prod_{j \in [n^2]} \mathbb{E} \left[\exp \{e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,j}, F_{l+2,j}, \dots, F_{k,j}), \mathbf{x}_{\mathcal{Q}})\} \middle| F_{\mathcal{Q},j_{\mathcal{Q}}} \right] \right] \quad (183)$$

$$\stackrel{(c)}{=} (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E}_{F_{\mathcal{Q},j_{\mathcal{Q}}}} \left[\left(\mathbb{E} \left[\exp \{e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,1}, F_{l+2,1}, \dots, F_{k,1}), \mathbf{x}_{\mathcal{Q}})\} \middle| F_{\mathcal{Q},j_{\mathcal{Q}}} \right] \right)^{n^2} \right] \quad (184)$$

$$\stackrel{(d)}{\leq} (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E}_{F_{\mathcal{Q},j_{\mathcal{Q}}}} \left[\left(1 + \mathbb{E} \left[e_{\mathcal{Q}}(F_{\mathcal{Q},j_{\mathcal{Q}}}, (F_{l+1,1}, F_{l+2,1}, \dots, F_{k,1}), \mathbf{x}_{\mathcal{Q}}) \middle| F_{\mathcal{Q},j_{\mathcal{Q}}} \right] \right)^{n^2} \right] \quad (185)$$

$$\stackrel{(e)}{\leq} (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \mathbb{E}_{F_{\mathcal{Q},j_{\mathcal{Q}}}} \left[\left(1 + P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi) \right)^{n^2} \right] \quad (186)$$

$$= (n^2)^{k-l-1} \exp \{-n^2 \epsilon\} \left(1 + P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi) \right)^{n^2} \quad (187)$$

$$= \exp \left\{ -n^2 \left(\epsilon - \log(1 + P_e^{\text{rand}}(P_{F_{[1:k]}}, \phi)) \right) - \frac{k-l-1}{n^2} \log(n^2) \right\}. \quad (188)$$

(a) If for any $i \in \mathcal{Q}^c$, $I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) \geq \epsilon$, then,

$$\frac{1}{N^{|\mathcal{Q}^c|}} |\{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c} : (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n\}| \\ < \exp\{-n\epsilon/2\}.$$

(b) If for any $i \in \mathcal{Q}^c$, $I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{T}}' X_{\mathcal{J}}' X_{\mathcal{Q}}) \geq (|\mathcal{T}| + |\mathcal{J}|)(1/n) \log_2 N + \epsilon$, then,

$$\frac{1}{N^{|\mathcal{Q}^c|}} |\{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c} : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}, m'_i \neq m_i, \forall i \in \mathcal{T}, (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), f_{\mathcal{T}}(m'_{\mathcal{T}}), f_{\mathcal{J}}(m'_{\mathcal{J}}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{T}}' X_{\mathcal{J}}' X_{\mathcal{Q}}}^n\}| \\ < \exp\{-n\epsilon/2\}.$$

Proof of Lemma 9: For $\epsilon > 0$ (fixed later), large enough $n, N \geq \exp(n\epsilon)$ and types $P_i \in \mathcal{P}_{\mathcal{X}_i}^n, i \in [1 : k]$, such that $\min_{i \in [1:k]} \min_{x_i \in \mathcal{X}_i} P_i > 0$, consider the codebooks $\mathcal{C}_i, i \in [1 : k]$ for message sets $\mathcal{M}_i = [1 : N], i \in [1 : k]$ as given by Lemma 15. The rates of the codebooks $R_i = R = \log_2(N)/n$ for some $R \geq \epsilon$. The decoder is given by Definition 10 for η satisfying Lemma 17. We will choose ϵ such that $\eta > (2k + 1)(k + 1)\epsilon$.

Let $\mathcal{Q} \in \mathcal{A}$ be the set of adversarial users who attack with input vector $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$. The probability of error is given by

$$\frac{1}{N^{|\mathcal{Q}^c|}} \sum_{m_{\mathcal{Q}^c}} \mathbb{P}(\{\mathbf{y} : \phi(\mathbf{y}) \neq (m_{\mathcal{Q}^c}, m_{\mathcal{Q}}) \text{ for some } m_{\mathcal{Q}}\} \\ |\mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}). \quad (192)$$

From the decoder definition (Definition 10), we know that if $\phi(\mathbf{y}) = \tilde{m}_{[1:k]}$ where $m_{\mathcal{Q}^c} \neq \tilde{m}_{\mathcal{Q}^c}$, then $\mathbf{y} \notin \cap_{i \in \mathcal{Q}^c} \mathcal{D}_{m_i}^{(i)}$, that

is, $\mathbf{y} \in \cup_{i \in \mathcal{Q}^c} (\mathcal{D}_{m_i}^i)^c$. Thus, (192) can be written as

$$\frac{1}{N^{|\mathcal{Q}^c|}} \sum_{m_{\mathcal{Q}^c}} \mathbb{P}(\{\mathbf{y} : \mathbf{y} \notin \cap_{i \in \mathcal{Q}^c} \mathcal{D}_{m_i}^{(i)}\} \\ |\mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \\ \leq \sum_{i \in \mathcal{Q}^c} \frac{1}{N^{|\mathcal{Q}^c|}} \sum_{m_{\mathcal{Q}^c}} \mathbb{P}(\{\mathbf{y} : \mathbf{y} \notin \mathcal{D}_{m_i}^{(i)}\} \\ |\mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}). \quad (193)$$

We will show that each term in (193) falls exponentially. It holds when for joint distribution $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}$ defined by $(f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n, I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) \geq \epsilon$ for any $i \in \mathcal{Q}^c$. This is because for any $j \in \mathcal{Q}^c$,

$$\frac{1}{N^{|\mathcal{Q}^c|}} \sum_{\substack{m_{\mathcal{Q}^c} : (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n, \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) \geq \epsilon \text{ for some } i \in \mathcal{Q}^c}} \mathbb{P}(\mathbf{y} : \mathbf{y} \notin \mathcal{D}_{m_j}^{(j)} | \mathbf{X}_{\mathcal{Q}^c} \\ = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \\ \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}: \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) \geq \epsilon \\ \text{for some } i \in \mathcal{Q}^c}} \frac{1}{N^{|\mathcal{Q}^c|}} |\{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c} : (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \\ \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n\}| \\ \stackrel{(a)}{<} \sum_{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}} \exp\{-n\epsilon/2\} \rightarrow 0,$$

where (a) follows from Lemma 15(a). Thus, we can assume that $I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon$ for all $i \in \mathcal{Q}^c$. This implies that

$$|\mathcal{Q}^c| \epsilon > \sum_{i \in \mathcal{Q}^c} I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}})$$

$$\begin{aligned} & P_{e, \mathcal{Q}}^{\text{rand}}(\tilde{f}_{[1:k]}, \tilde{\phi}) \\ &= \max_{\substack{(\hat{\mathbf{x}}_{\mathcal{Q}}, \mathbf{x}_{\mathcal{Q}}) \\ \in \mathcal{X}_{\mathcal{Q}}^{kn} \times \mathcal{X}_{\mathcal{Q}}^n}} \frac{1}{(\prod_{i \in \mathcal{Q}^c} \tilde{N}_i)} \sum_{\tilde{m}_{\mathcal{Q}^c} \in \tilde{\mathcal{M}}_{\mathcal{Q}^c}} \mathbb{P}\left(\left\{\tilde{\phi}(\tilde{\mathbf{Y}}) = m'_{[1:k]} \text{ such that } m'_{\mathcal{Q}^c} \neq \tilde{m}_{\mathcal{Q}^c}\right\} \middle| \tilde{\mathbf{X}}_{\mathcal{Q}^c} = \tilde{f}_{\mathcal{Q}^c}(\tilde{m}_{\mathcal{Q}^c}), \tilde{\mathbf{X}}_{\mathcal{Q}} = (\hat{\mathbf{x}}_{\mathcal{Q}}, \mathbf{x}_{\mathcal{Q}})\right) \\ &\leq \max_{\substack{\hat{\mathbf{x}}_{\mathcal{Q}}, \mathbf{x}_{\mathcal{Q}} \\ \in \mathcal{X}_{\mathcal{Q}}^{kn} \times \mathcal{X}_{\mathcal{Q}}^n}} \frac{1}{(n^2)^{|\mathcal{Q}^c|} (\prod_{i \in \mathcal{Q}^c} N_i)} \sum_{l_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}\left(\left\{\hat{\phi}(\hat{\mathbf{Y}}) = \bar{l}_{[1:k]} \text{ such that } \bar{l}_{\mathcal{Q}^c} \neq l_{\mathcal{Q}^c}\right\} \right. \\ &\quad \left. \cup \left\{\phi(\mathbf{Y}, f_{\mathcal{Q}, l_{\mathcal{Q}}}, f_{\mathcal{Q}^c, l_{\mathcal{Q}^c}}) = \bar{m}_{[1:k]} \text{ such that } \bar{m}_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}\right\} \right. \\ &\quad \left. \left| (\hat{\mathbf{X}}_{\mathcal{Q}^c}, \mathbf{X}_{\mathcal{Q}^c}) = (\hat{f}_{\mathcal{Q}^c}(l_{\mathcal{Q}^c}), f_{\mathcal{Q}^c, l_{\mathcal{Q}^c}}(m_{\mathcal{Q}^c})), (\hat{\mathbf{X}}_{\mathcal{Q}} = \hat{\mathbf{x}}_{\mathcal{Q}}, \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \right) \right. \\ &\leq \max_{\mathbf{x}_{\mathcal{Q}}} \frac{1}{(n^2)^{|\mathcal{Q}^c|}} \sum_{l_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} \mathbb{P}\left(\left\{\hat{\phi}(\hat{\mathbf{Y}}) = \bar{l}_{[1:k]} \text{ such that } \bar{l}_{\mathcal{Q}^c} \neq l_{\mathcal{Q}^c}\right\} \middle| \hat{\mathbf{X}}_{\mathcal{Q}^c} = \hat{f}_{\mathcal{Q}^c}(l_{\mathcal{Q}^c}), \hat{\mathbf{X}}_{\mathcal{Q}} = \hat{\mathbf{x}}_{\mathcal{Q}}\right) \\ &+ \max_{\mathbf{x}_{\mathcal{Q}}, l_{\mathcal{Q}}} \frac{1}{(n^2)^{|\mathcal{Q}^c|} (\prod_{i \in \mathcal{Q}^c} N_i)} \sum_{l_{\mathcal{Q}^c} \in [1:n^2]^{|\mathcal{Q}^c|}} \sum_{m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}} \mathbb{P}\left(\left\{\phi(\mathbf{Y}, f_{\mathcal{Q}, l_{\mathcal{Q}}}, f_{\mathcal{Q}^c, l_{\mathcal{Q}^c}}) = \bar{m}_{[1:k]} \text{ such that } \bar{m}_{\mathcal{Q}^c} \neq m_{\mathcal{Q}^c}\right\} \middle| \right. \\ &\quad \left. \mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c, l_{\mathcal{Q}^c}}(m_{\mathcal{Q}^c}), \mathbf{X}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}\right) \\ &\stackrel{(a)}{\leq} 2\epsilon. \end{aligned} \quad (191)$$

$$\geq D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} \right\| \right).$$

Under this case, for any $j \in \mathcal{Q}^c$,

$$\begin{aligned} & \frac{1}{N^{|\mathcal{Q}^c|}} \sum_{\substack{m_{\mathcal{Q}^c}: (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n, \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon \forall i \in \mathcal{Q}^c}} \mathbb{P}(\{\mathbf{y} : \mathbf{y} \notin \mathcal{D}_{m_j}^{(j)}\} \\ & \quad | \mathbf{X}_{\mathcal{Q}^c} = f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}} = \mathbf{x}_{\mathcal{Q}}) \quad (194) \\ & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon \forall i \in \mathcal{Q}^c}} \frac{1}{N^{|\mathcal{Q}^c|}} \sum_{\substack{m_{\mathcal{Q}^c}: \\ (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n}} \\ & \quad \sum_{y \in T_{Y|X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}})} W^n(y | f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \\ & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon \forall i \in \mathcal{Q}^c}} \frac{1}{N^{|\mathcal{Q}^c|}} \\ & \quad \sum_{m_{\mathcal{Q}^c}: (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n} \\ & \quad \exp \left\{ -n D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} W \right\| \right) \right\} \\ & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \forall i \in \mathcal{Q}^c, \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon}} \exp \left\{ -n D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} W \right\| \right) \right\} \\ & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \forall i \in \mathcal{Q}^c, \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon}} \\ & \quad \exp \left\{ -n \left(D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) \right. \right. \\ & \quad \left. \left. - D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} \right\| \right) \right) \right\}. \quad (195) \end{aligned}$$

We will break (195) into two terms, first corresponding to joint distributions $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y}$ for which

$$D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) \geq \eta$$

and second corresponding to joint distributions for which

$$D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) < \eta.$$

Let us start by considering the former.

$$\begin{aligned} & \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon, \forall i \in \mathcal{Q}^c}} \\ & D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) \geq \eta \\ & \exp \left\{ -n \left(D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) \right. \right. \\ & \quad \left. \left. - D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} \right\| \right) \right) \right\} \end{aligned}$$

$$\begin{aligned} & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}} : \\ I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X_{\mathcal{Q}}) < \epsilon \forall i \in \mathcal{Q}^c}} \exp \{ -n(\eta - |\mathcal{Q}^c| \epsilon) \} \\ & \rightarrow 0 \text{ for } \eta > k\epsilon. \end{aligned}$$

Now, we need to evaluate (195) for joint distributions $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y}$ for which $D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) < \eta$. In this case, since decoding condition 1 holds, $\mathbf{y} \notin \mathcal{D}_{m_j}^{(j)}$ if decoding condition 2 fails. That is, there exist $\mathcal{Q}' \in \mathcal{A}$, not necessarily distinct from \mathcal{Q} , a non-empty set $\mathcal{T} \subseteq (\mathcal{Q} \cup \mathcal{Q}')^c$ with $j \in \mathcal{T}$, $\mathbf{x}'_{\mathcal{Q}'} \in \mathcal{X}_{\mathcal{Q}'}^n$, $m'_{\mathcal{Q} \setminus \mathcal{Q}'} \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}$, $m'_T \in \mathcal{M}_{\mathcal{T}}$ such that $m'_t \neq m_t$ for all $t \in \mathcal{T}$ such that for the joint distribution $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} Y$ defined by $(f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}, f_T(m'_T), f_{\mathcal{Q} \setminus \mathcal{Q}'}(m'_{\mathcal{Q} \setminus \mathcal{Q}'}), \mathbf{x}'_{\mathcal{Q}'}, \mathbf{y}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} Y$,

$$\begin{aligned} & D \left(P_{X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X_{\mathcal{Q}^c \setminus (\mathcal{T} \cup \mathcal{Q}')}} X'_{\mathcal{Q}'} Y \right) \\ & \left(\prod_{t \in \mathcal{T}} P_{X'_t} \right) \left(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}'} P_{X'_j} \right) \left(\prod_{l \in \mathcal{Q}^c \setminus (\mathcal{T} \cup \mathcal{Q}')} P_{X_l} \right) P_{X'_{\mathcal{Q}'}} W \right) < \eta \\ & \text{and } I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} | X_{\mathcal{Q}}) \geq \eta. \end{aligned}$$

Let $\mathcal{H} := \mathcal{Q}^c \setminus (\mathcal{T} \cup \mathcal{Q}')$ and $\mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^1 Y$ be the set of distributions $P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} Y$ satisfying $D \left(P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} Y} \left\| \left(\prod_{i \in \mathcal{Q}^c} P_{X_i} \right) P_{X_{\mathcal{Q}}} W \right\| \right) \leq \eta$,

$$\begin{aligned} & D \left(P_{X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X_{\mathcal{H}} X'_{\mathcal{Q}'}} Y \right) \\ & \left(\prod_{t \in \mathcal{T}} P_{X'_t} \right) \left(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}'} P_{X'_j} \right) \left(\prod_{l \in \mathcal{H}} P_{X_l} \right) P_{X'_{\mathcal{Q}'}} W \right) < \eta, \end{aligned}$$

and $I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} | X_{\mathcal{Q}}) \geq \eta$. Using these definitions we see that, in this case, (194) is upper bounded by

$$\begin{aligned} & \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} Y \\ \in \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^1 Y}} \\ & \frac{1}{N^{|\mathcal{Q}^c|}} \left| \left\{ m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c} : \exists m'_{\mathcal{Q} \setminus \mathcal{Q}'} \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}, \right. \right. \\ & \quad \left. \left. m'_T \in \mathcal{M}_{\mathcal{T}} \text{ where } m'_t \neq m_t \text{ for all } t \in \mathcal{T} \text{ such that} \right. \right. \\ & \quad \left. \left. (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), f_T(m'_T), f_{\mathcal{Q} \setminus \mathcal{Q}'}(m'_{\mathcal{Q} \setminus \mathcal{Q}'}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^n \right\} \right| \\ & \leq \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} Y \\ \in \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^1 Y}} \exp \{ -n\epsilon/2 \} \\ & \rightarrow 0 \end{aligned}$$

if for any $i \in \mathcal{Q}^c$, $I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X_{\mathcal{Q}}) \geq (|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon$. This follows from the codebook property Lemma 15(b). Thus, we only need to consider joint distributions for which $I(X_i; X_{\mathcal{Q}^c \setminus \{i\}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X_{\mathcal{Q}}) < (|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon$ for all $i \in \mathcal{Q}^c$. This implies that $I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}}) \leq |\mathcal{Q}^c|((|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon)$. This is because $I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}}) \leq \sum_{i \in \mathcal{Q}^c} I(X_i; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}})$.

Let $\mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2 = \{P_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y} \in \mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^1 : I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_T | X_Q) \leq |\mathcal{Q}^c|(|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon\}$. So, for any $j \in \mathcal{Q}^c$, it is sufficient to analyze the upper bound in (196), shown at the bottom of the next page. From the definitions of $\mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2$ and $\mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^1$, we note that $I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_T | X_Q) \geq \eta$ and $I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_T | X_Q) \leq |\mathcal{Q}^c|(|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon$. This implies that

$$\begin{aligned} & \sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y} \in: \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2}} \exp \left\{ n(|\mathcal{Q} \setminus \mathcal{Q}'| + |\mathcal{T}|)R \right. \\ & \quad \left. - I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_T | X_Q) \right. \\ & \quad \left. + I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_T | X_Q) + \epsilon \right\} \\ & \leq \sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y} \in: \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2}} \exp \left\{ n(|\mathcal{Q} \setminus \mathcal{Q}'| + |\mathcal{T}|)R - \eta \right. \\ & \quad \left. + |\mathcal{Q}^c|(|\mathcal{T}| + |(\mathcal{Q} \setminus \mathcal{Q}')|)R + \epsilon) + \epsilon \right\} \\ & \leq 2^k \sum_{\substack{P_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y} \in: \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2}} \exp \{n(kR - \eta + k(kR + \epsilon) + \epsilon)\} \\ & = 2^k \sum_{\substack{P_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y} \in: \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_Q X'_T X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'} Y}^2}} \exp \{n((k + k^2)R - \eta + (k + 1)\epsilon)\} \\ & \rightarrow 0 \text{ for } R < \frac{\eta - (k + 1)\epsilon}{k + k^2}. \end{aligned}$$

Since $\eta > (2k + 1)(k + 1)\epsilon$, $\frac{\eta - (k + 1)\epsilon}{k + k^2} > 2\epsilon$. Thus, we can choose R between ϵ and 2ϵ . \square

Proof of Lemma 15: This proof is along the lines of [10, Lemma 2] and [22, Lemma 3]. We will generate the codebooks by a random experiment. For any $\mathcal{Q} \in \mathcal{A}$, $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$ and joint type $P_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q} \in \mathcal{P}_{\mathcal{X}_{\mathcal{Q}^c} \times \mathcal{X}_T \times \mathcal{X}_{\mathcal{J}} \times \mathcal{X}_Q}^n$, we will show that the probability that statement (b) does not hold, falls doubly exponentially in n . We will only analyze statement (b) as choosing $\mathcal{T} = \mathcal{J} = \emptyset$ in (b) will also imply that the probability that (a) does not hold also falls doubly exponentially. Since \mathcal{A} , $|\mathcal{X}_{\mathcal{Q}^c}^n|$ and $|\mathcal{P}_{\mathcal{X}_{\mathcal{Q}^c} \times \mathcal{X}_T \times \mathcal{X}_{\mathcal{J}} \times \mathcal{X}_Q}^n|$ grow at most exponentially in n , a union bound will imply the existence of codebooks satisfying (a) and (b). The proof will use [22, Lemma A1] which we restate here for a quick reference.

Lemma 16: [22, Lemma A1] Let Z_1, \dots, Z_N be arbitrary random variables, and let $f_j(Z_1, \dots, Z_j)$ be arbitrary with $0 \leq f_j \leq 1$, $j \in 1, \dots, N$. Then the condition

$$E[f_j(Z_1, \dots, Z_j) | Z_1, \dots, Z_{j-1}] \leq a, \quad j \in [1 : N],$$

implies that for any real number t ,

$$\mathbb{P} \left\{ \frac{1}{N} \sum_{j=1}^N f_j(Z_1, \dots, Z_j) > t \right\} \leq \exp \{ -N(t - a \log e) \}.$$

Let T_i^n , $i \in [1 : k]$ denote the type class of P_i . We generate independent random codebooks for each user. The codebook for user $i \in [1 : k]$, denoted by $\mathcal{C}_i = (\mathbf{X}_{i,1}, \mathbf{X}_{i,2}, \dots, \mathbf{X}_{i,N})$, consists of independent random vectors each distributed uniformly on T_i^n . Fix $\mathcal{Q} \in \mathcal{A}$, $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$ and a joint type $P_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}$ such that for every $i \in \mathcal{Q}^c$, $P_{X_i} = P_i$, for $t \in \mathcal{T}$, $P_{X'_t} = P_t$ and for $j \in \mathcal{J}$, $P_{X'_j} = P_j$ and $\mathbf{x}_{\mathcal{Q}} \in T_{\mathcal{Q}}^n$. We will analyze the probability that (b) does not hold under the randomness of codebook generation process. Note that the bound in (b) is non-trivial only when $\mathcal{Q}^c \neq \emptyset$. For any $l \in \mathcal{Q}^c$,

$$\begin{aligned} & \mathbb{P} \left(\frac{1}{N^{|\mathcal{Q}^c|}} \left| \left\{ m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c} : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \right. \right. \\ & \quad \left. \left. \left. m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}, m'_i \neq m_i \text{ for all } i \in \mathcal{T} \text{ such that } \right. \right. \right. \\ & \quad \left. \left. \left. (\mathbf{X}_{\mathcal{Q}^c, m_{\mathcal{Q}^c}}, \mathbf{X}_{\mathcal{T}, m'_{\mathcal{T}}}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}^n \right\} \right. \right. \\ & \quad \left. \left. \left. > \exp \{-n\epsilon/2\} \right\} \right. \right. \\ & = \mathbb{P} \left(\sum_{m_{\mathcal{Q}^c \setminus \{l\}} \in \mathcal{M}_{\mathcal{Q}^c \setminus \{l\}}} \frac{1}{N} \left| \left\{ m_l \in \mathcal{M}_l : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \right. \right. \\ & \quad \left. \left. \left. m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}, m'_i \neq m_i \text{ for all } i \in \mathcal{T} \text{ such that } \right. \right. \right. \\ & \quad \left. \left. \left. (\mathbf{X}_{\mathcal{Q}^c, m_{\mathcal{Q}^c}}, \mathbf{X}_{\mathcal{T}, m'_{\mathcal{T}}}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}^n \right\} \right. \right. \\ & \quad \left. \left. \left. > \exp \{-n\epsilon/2\} \right\} \right. \right. \\ & \leq \sum_{m_{\mathcal{Q}^c \setminus \{l\}} \in \mathcal{M}_{\mathcal{Q}^c \setminus \{l\}}} \mathbb{P} \left(\frac{1}{N} \left| \left\{ m_l \in \mathcal{M}_l : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \right. \right. \\ & \quad \left. \left. \left. m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}, m'_i \neq m_i \text{ for all } i \in \mathcal{T} \text{ such that } \right. \right. \right. \\ & \quad \left. \left. \left. (\mathbf{X}_{\mathcal{Q}^c, m_{\mathcal{Q}^c}}, \mathbf{X}_{\mathcal{T}, m'_{\mathcal{T}}}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}^n \right\} \right. \right. \\ & \quad \left. \left. \left. > \exp \{-n\epsilon/2\} \right\} \right. \right. \\ & \leq \sum_{\substack{m_{\mathcal{Q}^c \setminus \{l\}} \in \mathcal{M}_{\mathcal{Q}^c \setminus \{l\}} \\ \in \mathcal{M}_{\mathcal{Q}^c \setminus \{l\}} \in T_{X_{\mathcal{Q}^c \setminus \{l\}} | X_{\mathcal{Q}}}^n(\mathbf{x}_{\mathcal{Q}})}} \left(\sum_{\mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}} \mathbb{P}(\mathbf{X}_{\mathcal{Q}^c \setminus \{l\}, m_{\mathcal{Q}^c \setminus \{l\}}} = \mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}) \right. \\ \left. \mathbb{P} \left(\frac{1}{N} \left| \left\{ m_l \in \mathcal{M}_l : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \right. \right. \right. \\ \left. \left. \left. m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}, m'_i \neq m_i \text{ for all } i \in \mathcal{T} \text{ such that } \right. \right. \right. \\ \left. \left. \left. (\mathbf{X}_{l, m_l}, \mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}, \mathbf{X}_{\mathcal{T}, m'_{\mathcal{T}}}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}^n \right\} \right. \right. \\ \left. \left. \left. > \exp \{-n\epsilon/2\} \right\} \right. \right. \right). \end{aligned} \tag{197}$$

To analyze this, we first consider the case when $\mathcal{T} \neq \emptyset$. Recall that $\mathcal{T} \subseteq \mathcal{Q}^c$. Without loss of generality, suppose $1 \in \mathcal{Q}^c \cap \mathcal{T}$. Then for $l = 1$, we have (198)–(200), shown at the bottom of the next page.

We will now analyze (199) using Lemma 16. For $j \in [1 : N]$, let $Z_j = (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]})$ where the codewords for $m_{\mathcal{Q}^c \setminus \{l\}}$ are fixed to $\mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}$. Let $f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j)$ be defined as

$$\begin{aligned} & f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) \\ & = f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}}((\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]})) \\ & = \begin{cases} 1, & \text{if } \exists i < j, (m'_{\mathcal{T} \setminus \{1\}}, m'_{\mathcal{J}}) \in \mathcal{M}_{\mathcal{T} \setminus \{1\}} \times \mathcal{M}_{\mathcal{J}} \\ & \text{such that } \forall t \in \mathcal{T} \setminus \{1\}, m'_t \neq m_t, \\ & ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{l\}}), (\mathbf{X}_{1,i}, \mathbf{X}_{(\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}})}), \\ & \mathbf{X}_{(\mathcal{J}, m'_{\mathcal{J}})}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_T X'_{\mathcal{J}} X_Q}^n, \\ & 0, & \text{otherwise.} \end{cases} \end{aligned}$$

For $t = \frac{1}{2} \exp\{-n\epsilon/2\}$, (199) can be written as

$$\left(\frac{1}{N} \sum_{j=1}^N f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) > t \right)$$

We will compute a in Lemma 16.

$$\mathbb{E} \left[f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}((\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]})) \right. \\ \left. | (\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,(j-1)}, \mathcal{C}_{[2:k]}) \right]$$

$$\leq \sum_{\substack{i \in \mathcal{M}_1, i < j \\ (m'_{\mathcal{T} \setminus \{1\}}, m'_{\mathcal{J}}) \in \mathcal{M}_{\mathcal{T} \setminus \{1\}} \times \mathcal{M}_{\mathcal{J}} \\ m'_t \neq m_t, t \in \mathcal{T} \setminus \{1\}}} \mathbb{P} \left(((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), \right. \\ \left. (\mathbf{X}_{1,i}, \mathbf{X}_{(\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}})}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \right. \\ \left. | (\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,(j-1)}, \mathcal{C}_{[2:k]}) \right) \\ \leq N^{(|\mathcal{T}|+|\mathcal{J}|)} \frac{\exp\{nH(X_1 | X_{\mathcal{Q}^c \setminus \{1\}} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}})\}}{(n+1)^{-|\mathcal{X}_1|} \exp\{nH(X_1)\}} \\ = (n+1)^{|\mathcal{X}_1|} \exp \left\{ n((|\mathcal{T}|+|\mathcal{J}|)(1/n) \log_2 N \right. \\ \left. - I(X_1; X_{\mathcal{Q}^c \setminus \{1\}} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}) \right\}$$

$$\sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^2}} \frac{1}{N^{|\mathcal{Q}^c|}} \sum_{\substack{m_{\mathcal{Q}^c}: \\ (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n}} \sum_{\substack{y \in T_{Y | X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n \\ \mathbf{y} \notin \mathcal{D}_{m_j}^{(j)}}} W^n(y | f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \\ \leq \sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^2}} \frac{1}{N^{|\mathcal{Q}^c|}} \sum_{\substack{m_{\mathcal{Q}^c}: \\ (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n}} \sum_{\substack{m'_{\mathcal{Q} \setminus \mathcal{Q}'} \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'} \\ m'_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}} \\ (f_{\mathcal{Q} \setminus \mathcal{Q}'}(m'_{\mathcal{Q} \setminus \mathcal{Q}'}), f_{\mathcal{T}}(m'_{\mathcal{T}})) \in T_{X_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n \\ (f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X_{\mathcal{Q}}}^n}} W^n(y | f_{\mathcal{Q}^c}(m_{\mathcal{Q}^c}), \mathbf{x}_{\mathcal{Q}}) \\ \leq \sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^2}} \exp \left\{ n(|\mathcal{Q} \setminus \mathcal{Q}'| + |\mathcal{T}|)R - I(Y; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}^c} X_{\mathcal{Q}}) + \epsilon \right\} \\ = \sum_{\mathcal{Q}' \in \mathcal{A}} \sum_{\substack{P_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}} \\ \mathcal{P}_{X_{\mathcal{Q}^c} X_{\mathcal{Q}} X'_{\mathcal{T}} X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{Q}'}}^2}} \exp \left\{ n(|\mathcal{Q} \setminus \mathcal{Q}'| + |\mathcal{T}|)R - I(X_{\mathcal{Q}^c} Y; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}}) + I(X_{\mathcal{Q}^c}; X'_{\mathcal{Q} \setminus \mathcal{Q}'} X'_{\mathcal{T}} | X_{\mathcal{Q}}) + \epsilon \right\} \quad (196)$$

$$\mathbb{P} \left(\frac{1}{N} |\{m_1 \in \mathcal{M}_1 : \exists m'_T \in \mathcal{M}_T, m'_t \neq m_t \text{ for all } t \in \mathcal{T}, m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \\ \left. ((\mathbf{X}_{1,m_1}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), \mathbf{X}_{\mathcal{T}, m'_T}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \} | > \exp\{-n\epsilon/2\} \right) \\ = \mathbb{P} \left(\frac{1}{N} |j \in \mathcal{M}_1 : \exists i < j, i \in \mathcal{M}_1, m'_{\mathcal{T} \setminus \{1\}} \in \mathcal{M}_{\mathcal{T} \setminus \{1\}}, m'_t \neq m_t \text{ for all } t \in \mathcal{T} \setminus \{1\}, m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \\ \left. ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), (\mathbf{X}_{1,i}, \mathbf{X}_{\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}}}), \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \} | \right. \\ \left. + \frac{1}{N} |j \in \mathcal{M}_1 : \exists i > j, i \in \mathcal{M}_1, m'_{\mathcal{T} \setminus \{1\}} \in \mathcal{M}_{\mathcal{T} \setminus \{1\}}, m'_t \neq m_t \text{ for all } t \in \mathcal{T} \setminus \{1\}, m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \\ \left. ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), (\mathbf{X}_{1,i}, \mathbf{X}_{\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}}}), \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \} | > \exp\{-n\epsilon/2\} \right) \quad (198)$$

$$\leq \mathbb{P} \left(\frac{1}{N} |j \in \mathcal{M}_1 : \exists i < j, i \in \mathcal{M}_1, m'_{\mathcal{T} \setminus \{1\}} \in \mathcal{M}_{\mathcal{T} \setminus \{1\}}, m'_t \neq m_t \text{ for all } t \in \mathcal{T} \setminus \{1\}, m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \\ \left. ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), (\mathbf{X}_{1,i}, \mathbf{X}_{\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}}}), \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \} | > \frac{1}{2} \exp\{-n\epsilon/2\} \right) \quad (199)$$

$$+ \mathbb{P} \left(\frac{1}{N} |j \in \mathcal{M}_1 : \exists i > j, i \in \mathcal{M}_1, m'_{\mathcal{T} \setminus \{1\}} \in \mathcal{M}_{\mathcal{T} \setminus \{1\}}, m'_t \neq m_t \text{ for all } t \in \mathcal{T} \setminus \{1\}, m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, \right. \\ \left. ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), (\mathbf{X}_{1,i}, \mathbf{X}_{\mathcal{T} \setminus \{1\}, m'_{\mathcal{T} \setminus \{1\}}}), \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{T}} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n \} | > \frac{1}{2} \exp\{-n\epsilon/2\} \right). \quad (200)$$

Suppose $I(X_1; X_{\mathcal{Q}^c \setminus \{1\}} X'_T X'_{\mathcal{J}} X_{\mathcal{Q}}) > (|\mathcal{T}| + |\mathcal{J}|)(1/n) \log_2 N + \epsilon$. Then, $a = (n+1)^{|\mathcal{X}_1|} \exp\{-n\epsilon\}$. Thus,

$$\begin{aligned} & \left(\frac{1}{N} \sum_{j=1}^N f_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) > t \right) \\ & \leq \exp\{-N(t - a \log_2 e)\} \\ & = \exp\left\{-N\left(\frac{1}{2} \exp\{-n\epsilon/2\} - (n+1)^{|\mathcal{X}_1|} \exp\{-n\epsilon\}\right)\right\} \\ & \leq \exp\left\{\left(-\frac{1}{2} \exp\{n\epsilon/2\} + (n+1)^{|\mathcal{X}_1|}\right)\right\} \end{aligned}$$

because $N \leq \exp\{n\epsilon\}$.

Thus, (199) falls doubly exponentially. Since (200) is symmetric to (199), we can obtain the same upper bound for (200) as well. This implies that (197) falls doubly exponentially when $\mathcal{T} \neq \emptyset$. Now, we consider the case when $\mathcal{T} = \emptyset$. In this case, in order to show that (197) falls doubly exponentially, we need to show that

$$\mathbb{P}\left(\frac{1}{N} \left| \{m_l \in \mathcal{M}_l : \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}, (\mathbf{X}_{l, m_l}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}, \mathbf{X}_{\mathcal{J}, m'_{\mathcal{J}}}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n\} \right| > \exp\{-n\epsilon/2\}\right) \quad (201)$$

falls doubly exponentially. This can be shown in a similar manner as the previous case. Again, without loss of generality, suppose $l = 1$. Let $Z_j = (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]}), j \in [1:N]$, where the codewords $\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}$ corresponding to messages $m_{\mathcal{Q}^c \setminus \{1\}}$ are fixed. Let $g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j)$ be defined as

$$\begin{aligned} g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) &= g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}((\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]})) \\ &= \begin{cases} 1 & \text{if } \exists m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}} \text{ such that} \\ & ((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), \mathbf{X}_{(\mathcal{J}, m'_{\mathcal{J}})}, \mathbf{x}_{\mathcal{Q}}) \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

For $t = \exp\{-n\epsilon/2\}$, (201) is

$$\mathbb{P}\left(\frac{1}{N} \sum_{j=1}^N g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) > t\right).$$

Computing a ,

$$\begin{aligned} & \mathbb{E}\left[g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}((\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,j}, \mathcal{C}_{[2:k]}))\right] \\ & \leq \sum_{m'_{\mathcal{J}} \in \mathcal{M}_{\mathcal{J}}} \mathbb{P}\left((\mathbf{X}_{1,j}, \mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}), \mathbf{X}_{(\mathcal{J}, m'_{\mathcal{J}})}, \mathbf{x}_{\mathcal{Q}} \in T_{X_{\mathcal{Q}^c} X'_{\mathcal{J}} X_{\mathcal{Q}}}^n | (\mathbf{X}_{1,1}, \mathcal{C}_{[2:k]}), \dots, (\mathbf{X}_{1,(j-1)}, \mathcal{C}_{[2:k]})\right) \\ & \leq N^{|\mathcal{J}|} \frac{\exp\{nH(X_1 | X_{\mathcal{Q}^c \setminus \{1\}} X'_{\mathcal{J}} X_{\mathcal{Q}})\}}{(n+1)^{-|\mathcal{X}_1|} \exp\{nH(X_1)\}} \\ & = (n+1)^{|\mathcal{X}_1|} \exp\left\{n(|\mathcal{J}|)(1/n) \log_2 N - I(X_1; X_{\mathcal{Q}^c \setminus \{1\}} X'_{\mathcal{J}} X_{\mathcal{Q}})\right\} \end{aligned}$$

Suppose $I(X_1; X_{\mathcal{Q}^c \setminus \{1\}} X'_{\mathcal{J}} X_{\mathcal{Q}}) > (|\mathcal{J}|)(1/n) \log_2 N + \epsilon$. Then, $a = (n+1)^{|\mathcal{X}_1|} \exp\{-n\epsilon\}$. Thus,

$$\begin{aligned} & \left(\frac{1}{N} \sum_{j=1}^N g_j^{\mathbf{x}_{\mathcal{Q}^c \setminus \{1\}}}(\mathbf{Z}_1, \dots, \mathbf{Z}_j) > t \right) \\ & \leq \exp\{-N(t - a \log_2 e)\} \\ & = \exp\left\{-N\left(\exp\{-n\epsilon/2\} - (n+1)^{|\mathcal{X}_1|} \exp\{-n\epsilon\}\right)\right\} \\ & \leq \exp\left\{-\left(\exp\{n\epsilon/2\} + (n+1)^{|\mathcal{X}_1|}\right)\right\} \end{aligned}$$

which falls doubly exponentially. \square

Lemma 17: Suppose the Byzantine MAC (W, \mathcal{A}) is not symmetrizable. Let $P_i \in \mathcal{P}_{\mathcal{X}_i}, i \in [1:k]$ be distributions such that $P_i(x_i) > 0, x_i \in \mathcal{X}_i, i \in [1:k]$. Let $f_i : \mathcal{M}_i \rightarrow T_{X_i}^n, i \in [1:k]$ be some encoding maps. There exists a choice of $\eta > 0$ such that if $(m_1, m_2, \dots, m_k) \neq (\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_k)$, $\mathcal{D}_{m_1, m_2, \dots, m_k} \cap \mathcal{D}_{\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_k} = \emptyset$.

Proof: Suppose for $(\hat{m}_1, \hat{m}_2, \dots, \hat{m}_k) \neq (\bar{m}_1, \bar{m}_2, \dots, \bar{m}_k)$, there exists $\mathbf{y} \in \mathcal{D}_{\hat{m}_1, \hat{m}_2, \dots, \hat{m}_k} \cap \mathcal{D}_{\bar{m}_1, \bar{m}_2, \dots, \bar{m}_k}$. This implies that there exists $\gamma \in [1:k]$ such that $\mathbf{y} \in \mathcal{D}_{\hat{m}_\gamma}^{(\gamma)} \cap \mathcal{D}_{\bar{m}_\gamma}^{(\gamma)}$ for $\hat{m}_\gamma \neq \bar{m}_\gamma$. Then, by the decoder definition, there exist $\mathcal{Q}, \tilde{\mathcal{Q}} \in \mathcal{A}$, not necessarily distinct, with $\gamma \notin \mathcal{Q}, \tilde{\mathcal{Q}}$; $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n, \tilde{\mathbf{x}}_{\tilde{\mathcal{Q}}} \in \mathcal{X}_{\tilde{\mathcal{Q}}}^n; m_{\mathcal{Q}^c} \in \mathcal{M}_{\mathcal{Q}^c}; \tilde{m}_{\tilde{\mathcal{Q}}^c} \in \mathcal{M}_{\tilde{\mathcal{Q}}^c}$ with $m_\gamma = \hat{m}_\gamma$ and $\tilde{m}_\gamma = \bar{m}_\gamma$ such that for $\mathcal{T} := \{i \in (\mathcal{Q} \cup \tilde{\mathcal{Q}})^c : m_i \neq \tilde{m}_i\}$ (note that $\gamma \in \mathcal{T}$), and for the joint distributions $P_{X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} X_{\mathcal{Q}} Y}$ and $P_{\tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} \tilde{X}_{\tilde{\mathcal{Q}}} Y}$ defined by $(f_T(m_{\mathcal{T}}), f_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}}(m_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}}), f_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c}(m_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c}), \mathbf{x}_{\mathcal{Q}}, \mathbf{y}) \in T_{X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} X_{\mathcal{Q}} Y}$ and $(f_T(\tilde{m}_{\mathcal{T}}), f_{\mathcal{Q} \setminus \tilde{\mathcal{Q}}}(m_{\mathcal{Q} \setminus \tilde{\mathcal{Q}}}), f_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c}(m_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c}), \tilde{\mathbf{x}}_{\tilde{\mathcal{Q}}}, \mathbf{y}) \in T_{\tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} \tilde{X}_{\tilde{\mathcal{Q}}} Y}$ respectively, the following holds.

$$\begin{aligned} & D\left(P_{X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} X_{\mathcal{Q}} Y} \middle\| \left(\prod_{i \in \mathcal{T}} P_i\right) \left(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}} P_j\right) \right. \\ & \quad \left. \left(\prod_{l \in (\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} P_l\right) P_{X_{\mathcal{Q}}} W\right) < \eta, \end{aligned} \quad (202)$$

$$\begin{aligned} & D\left(P_{\tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} \tilde{X}_{\tilde{\mathcal{Q}}} Y} \middle\| \left(\prod_{i \in \mathcal{T}} P_i\right) \left(\prod_{j \in \mathcal{Q} \setminus \tilde{\mathcal{Q}}} P_j\right) \right. \\ & \quad \left. \left(\prod_{l \in (\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} P_l\right) P_{\tilde{X}_{\tilde{\mathcal{Q}}}} W\right) < \eta. \end{aligned} \quad (203)$$

Then, the decoding condition 2 implies that

$$I(X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} X_{\mathcal{Q}} Y; \tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}} | X_{\mathcal{Q}}) < \eta, \quad (204)$$

$$I(\tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} Y; X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} | \tilde{X}_{\tilde{\mathcal{Q}}}) < \eta. \quad (205)$$

For ease of notation, let $\mathcal{H} := (\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c$. From (203), by the chain rule of relative entropy, we get $D(P_{\tilde{X}_T \tilde{X}_{\mathcal{Q} \setminus \mathcal{Q}}} || (\prod_{i \in \mathcal{T}} P_i)(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}} P_j)) < \eta$. Using this, (202) and (204), we get

$$3\eta >$$

$$D(P_{X_T X_{\tilde{\mathcal{Q}} \setminus \mathcal{Q}} X'_{(\mathcal{T} \cup \mathcal{Q} \cup \tilde{\mathcal{Q}})^c} X_{\mathcal{Q}} Y} || (\prod_{i \in \mathcal{T}} P_i)(\prod_{j \in \mathcal{Q} \setminus \mathcal{Q}} P_j)(\prod_{l \in \mathcal{H}} P_l) P_{X_{\mathcal{Q}}} W)$$

$$\begin{aligned}
& + D(P_{\tilde{X}_T, \tilde{X}_{Q \setminus \tilde{Q}}} \parallel (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in Q \setminus \tilde{Q}} P_j)) \\
& + I(X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} Y; \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} | X_Q) \\
= & D(P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} X_Q Y} \parallel (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in \tilde{Q} \setminus Q} P_j) (\prod_{l \in \mathcal{H}} P_l) P_{X_Q} W) \\
& + D(P_{\tilde{X}_T, \tilde{X}_{Q \setminus \tilde{Q}}} \parallel (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in Q \setminus \tilde{Q}} P_j)) \\
& + D(P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} X_Q \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} Y} \\
& \quad P_{\tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} P_{X_Q | \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} Y | X_Q}) \\
= & D(P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} X_Q \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} Y} \parallel (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in \tilde{Q} \setminus Q} P_j) (\prod_{l \in \mathcal{H}} P_l) \\
& \quad (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in Q \setminus \tilde{Q}} P_j) P_{X_Q | \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} W_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} X_Q}) \\
\stackrel{(b)}{\geq} & D(P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} Y} \parallel (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in \tilde{Q} \setminus Q} P_j) (\prod_{l \in \mathcal{H}} P_l) \\
& \quad (\prod_{i \in \mathcal{T}} P_i) (\prod_{j \in Q \setminus \tilde{Q}} P_j) V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}})
\end{aligned}$$

$$\begin{aligned}
& \text{where } V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) \\
= & \sum_{x_Q} P_{X_Q | \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (x_Q | \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) W(y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, x_Q),
\end{aligned}$$

and (b) follows from the chain rule of relative entropy. Using Pinsker's inequality, it follows that

$$\begin{aligned}
& \sum_{x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, y} |P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} Y} (x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, y) - \\
& (\prod_{i \in \mathcal{T}} P_i(x_i)) (\prod_{j \in \tilde{Q} \setminus Q} P_j(x_j)) (\prod_{l \in \mathcal{H}} P_l(x'_l)) (\prod_{i \in \mathcal{T}} P_l(\tilde{x}_i)) (\prod_{j \in Q \setminus \tilde{Q}} P_j(\tilde{x}_j)) \\
& V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}})| \\
\leq & c\sqrt{3\eta}, \tag{206}
\end{aligned}$$

where c is some positive constant. By a symmetric analysis, we can show that

$$\begin{aligned}
& \sum_{x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, y} |P_{X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}} Y} (x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, y) - \\
& - (\prod_{i \in \mathcal{T}} P_i(x_i)) (\prod_{j \in \tilde{Q} \setminus Q} P_j(x_j)) (\prod_{l \in \mathcal{H}} P_l(x'_l)) (\prod_{i \in \mathcal{T}} P_l(\tilde{x}_i)) \\
& \quad (\prod_{j \in Q \setminus \tilde{Q}} P_j(\tilde{x}_j)) \\
& V'_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}})| \\
\leq & c\sqrt{3\eta}, \tag{207}
\end{aligned}$$

for

$$\begin{aligned}
& V'_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) = \\
& \sum_{\tilde{x}_{\tilde{Q}}} P_{\tilde{X}_{\tilde{Q}} | X_T X_{\tilde{Q} \setminus Q}} (\tilde{x}_{\tilde{Q}} | x_T, x_{\tilde{Q} \setminus Q}) W(y | \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, x'_{\mathcal{H}}, \tilde{x}_{\tilde{Q}}).
\end{aligned}$$

By (206) and (207),

$$\begin{aligned}
& \sum_{\substack{x_T, x_{\tilde{Q} \setminus Q}, i \in \mathcal{T} \\ x'_{\mathcal{H}}, \tilde{x}_T, \\ \tilde{x}_{Q \setminus \tilde{Q}}, y}} (\prod_{i \in \mathcal{T}} P_i(x_i)) (\prod_{j \in \tilde{Q} \setminus Q} P_j(x_j)) (\prod_{l \in \mathcal{H}} P_l(x'_l)) (\prod_{i \in \mathcal{T}} P_l(\tilde{x}_i)) \\
& \quad (\prod_{j \in Q \setminus \tilde{Q}} P_j(\tilde{x}_j)) \\
& |V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) \\
& \quad - V'_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}})| \\
\leq & 2c\sqrt{3\eta}.
\end{aligned}$$

This implies that for $\alpha := \min_{i \in [1:k]} \min_{x_i} P_i(x_i)$ (note that $\alpha > 0$),

$$\begin{aligned}
& \max_{\substack{x_T, x_{\tilde{Q} \setminus Q}, \\ x'_{\mathcal{H}}, \tilde{x}_T, \\ \tilde{x}_{Q \setminus \tilde{Q}}, y}} |V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) \\
& \quad - V'_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}})| \\
\leq & \frac{2c\sqrt{3\eta}}{\alpha^j} \tag{208}
\end{aligned}$$

for some integer j . Since (W, \mathcal{A}) is not symmetrizable, there exist $\zeta > 0$ such that

$$\begin{aligned}
& \max_{\substack{x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \\ \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, y}} \\
& \left| \sum_{x_Q} P_{X_Q | \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (x_Q | \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) W(y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, x_Q) \right. \\
& \left. - \sum_{\tilde{x}_{\tilde{Q}}} P_{\tilde{X}_{\tilde{Q}} | X_T X_{\tilde{Q} \setminus Q}} (\tilde{x}_{\tilde{Q}} | x_T, x_{\tilde{Q} \setminus Q}) W(y | \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}, x'_{\mathcal{H}}, \tilde{x}_{\tilde{Q}}) \right| \\
& > \zeta.
\end{aligned}$$

That is

$$\begin{aligned}
& \max_{\substack{x_T, x_{\tilde{Q} \setminus Q}, \\ x'_{\mathcal{H}}, \tilde{x}_T, \\ \tilde{x}_{Q \setminus \tilde{Q}}, y}} |V_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}}) \\
& \quad - V'_{Y | X_T X_{\tilde{Q} \setminus Q} X'_{\mathcal{H}} \tilde{X}_T \tilde{X}_{Q \setminus \tilde{Q}}} (y | x_T, x_{\tilde{Q} \setminus Q}, x'_{\mathcal{H}}, \tilde{x}_T, \tilde{x}_{Q \setminus \tilde{Q}})| \\
& > \zeta.
\end{aligned}$$

This contradicts (208) for choice of η and α satisfying $\frac{2c\sqrt{3\eta}}{\alpha^j} < \zeta$. \square

APPENDIX VIII PROOF OF THE CONVERSE OF THEOREM 8

Proof: Suppose the given byzantine-MAC (W, \mathcal{A}) is symmetrizable. Then, there exist $\mathcal{T} \subseteq [1:k]$, $\mathcal{Q}, \mathcal{Q}' \in \mathcal{A}$, not necessarily distinct, satisfying $\mathcal{Q} \cap \mathcal{T} = \mathcal{Q}' \cap \mathcal{T} = \emptyset$, and a pair of conditional distributions $P_{X_Q | X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}$ and $P'_{X_Q | X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}$ satisfying (209) below:

$$\begin{aligned}
& \sum_{x'_Q \in \mathcal{X}_Q} P_{X_Q | X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}} (x'_Q | x_T, x_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q})}) \\
& W(y | x'_Q, \tilde{x}_T, x_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q})}, x_{(\mathcal{T} \cup \mathcal{Q} \cup \mathcal{Q}')^c})
\end{aligned}$$

$$= \sum_{\tilde{x}_{\mathcal{Q}'} \in \mathcal{X}_{\mathcal{Q}'}} P'_{X_{\mathcal{Q}'}|X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}(\tilde{x}_{\mathcal{Q}'}|\tilde{x}_{\mathcal{T}}, x_{\mathcal{Q}' \setminus \mathcal{Q}}) \\ W(y|\tilde{x}_{\mathcal{Q}'}, x_{\mathcal{T}}, x_{\mathcal{Q} \setminus \mathcal{Q}'}, x_{(\mathcal{T} \cup \mathcal{Q} \cup \mathcal{Q}')^c}) \quad (209)$$

for every $y, x_{\mathcal{T}}, x_{\mathcal{Q} \setminus \mathcal{Q}'}, x_{(\mathcal{T} \cup \mathcal{Q} \cup \mathcal{Q}')^c}, \tilde{x}_{\mathcal{T}}$ and $x_{\mathcal{Q}' \setminus \mathcal{Q}}$. Let $m_{\mathcal{T}}, \tilde{m}_{\mathcal{T}} \in \mathcal{M}_3$ be such that $m_i \neq \tilde{m}_i$ for all $i \in \mathcal{T}$. We consider two different scenarios in which users in set \mathcal{T} send $f_{\mathcal{T}}(m_{\mathcal{T}})$ and $f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}})$ respectively:

(i) In the first setting, users in the set \mathcal{Q} are adversarial. They choose a message tuple $M_{\mathcal{Q} \setminus \mathcal{Q}'} \sim \text{Unif}(\mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'})$. Let $\mathbf{X}_{\mathcal{Q} \setminus \mathcal{Q}'} = f_{\mathcal{Q} \setminus \mathcal{Q}'}(M_{\mathcal{Q} \setminus \mathcal{Q}'})$. To produce their input $\mathbf{X}'_{\mathcal{Q}, m_{\mathcal{T}}}$ to the channel, they pass $(f_{\mathcal{T}}(m_{\mathcal{T}}), \mathbf{X}_{\mathcal{Q} \setminus \mathcal{Q}'})$ through $P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}^n$, the n -fold product of the channel $P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}^n$. Users in the set $(\mathcal{T} \cup \mathcal{Q})^c$, being non-adversarial, send as their input to the channel $\mathbf{X}_{(\mathcal{T} \cup \mathcal{Q})^c} = f_{(\mathcal{T} \cup \mathcal{Q})^c}(M_{(\mathcal{T} \cup \mathcal{Q})^c})$, where $M_{(\mathcal{T} \cup \mathcal{Q})^c} \sim \text{Unif}(\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q})^c})$. Users in the set \mathcal{T} send $f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}})$. The probability of any vector \mathbf{y} under this scenario is given by (210), shown at the bottom of the page, where $e_{\mathcal{Q}, \mathcal{T}}(\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}}, \mathbf{x}_{\mathcal{Q}})$ denotes

$$\frac{1}{|\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q})^c}|} \sum_{m_{(\mathcal{T} \cup \mathcal{Q})^c} \in \mathcal{M}_{(\mathcal{T} \cup \mathcal{Q})^c}} W^n(\bar{\mathbf{y}} \mid \mathbf{x}_{\mathcal{Q}}, f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}}), \\ f_{(\mathcal{T} \cup \mathcal{Q})^c}(m_{(\mathcal{T} \cup \mathcal{Q})^c}))$$

for $\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}$ and $\mathbf{x}_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n$. The notation \mathbf{y}_t represents the t^{th} component of the vector \mathbf{y} and for any set \mathcal{S} and message tuple $m_{\mathcal{S}} \in \mathcal{M}_{\mathcal{S}}$, $f_{\mathcal{S}, t}(m_{\mathcal{S}})$ and $\mathbf{x}_{\mathcal{S}, t}$ represents the $|\mathcal{S}|$ -length tuple containing the t^{th} components of the vectors in $f_{\mathcal{S}}(m_{\mathcal{S}})$ and $\mathbf{x}_{\mathcal{S}}$ respectively.

(ii) In the second setting, users in the set \mathcal{Q}' are adversarial. They choose a message tuple $M_{\mathcal{Q}' \setminus \mathcal{Q}} \sim \text{Unif}(\mathcal{M}_{\mathcal{Q}' \setminus \mathcal{Q}})$. Let $\mathbf{X}_{\mathcal{Q}' \setminus \mathcal{Q}} = f_{\mathcal{Q}' \setminus \mathcal{Q}}(M_{\mathcal{Q}' \setminus \mathcal{Q}})$. To produce their input $\tilde{\mathbf{X}}_{\mathcal{Q}', \tilde{m}_{\mathcal{T}}}$ to the channel, they pass $(f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}}), \mathbf{X}_{\mathcal{Q}' \setminus \mathcal{Q}})$ through $P_{X_{\mathcal{Q}'}|X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}^n$, the n -fold product of the channel $P'_{X_{\mathcal{Q}'}|X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}$. Users in the set $(\mathcal{T} \cup \mathcal{Q}')^c$, being non-adversarial, send $\mathbf{X}_{(\mathcal{T} \cup \mathcal{Q}')^c} = f_{(\mathcal{T} \cup \mathcal{Q}')^c}(M_{(\mathcal{T} \cup \mathcal{Q}')^c})$

as their input to the channel, where $M_{(\mathcal{T} \cup \mathcal{Q}')^c} \sim \text{Unif}(\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c})$. Users in the set \mathcal{T} send $f_{\mathcal{T}}(m_{\mathcal{T}})$. The probability of any vector \mathbf{y} under this scenario is given by (211), shown at the top of the next page, where $e_{\mathcal{Q}', \mathcal{T}}(\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}}, \mathbf{x}_{\mathcal{Q}'})$ denotes

$$\frac{1}{|\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}|} \sum_{m_{(\mathcal{T} \cup \mathcal{Q}')^c} \in \mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}} W^n(\bar{\mathbf{y}} \mid \mathbf{x}_{\mathcal{Q}'}, f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}}), \\ f_{(\mathcal{T} \cup \mathcal{Q}')^c}(m_{(\mathcal{T} \cup \mathcal{Q}')^c}))$$

for $\bar{\mathbf{y}} \in \mathcal{Y}^n$, $\tilde{m}_{\mathcal{T}} \in \mathcal{M}_{\mathcal{T}}$ and $\mathbf{x}_{\mathcal{Q}'} \in \mathcal{X}_{\mathcal{Q}'}^n$.

Note that

$$\mathbb{E}_{\tilde{\mathbf{X}}_{\mathcal{Q}', \tilde{m}_{\mathcal{T}}}} [e_{\mathcal{Q}', \mathcal{T}}(\bar{\mathbf{y}}, m_{\mathcal{T}}, \tilde{\mathbf{X}}_{\mathcal{Q}', \tilde{m}_{\mathcal{T}}})] \\ = \frac{1}{|\mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}|} \sum_{m_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c} \in \mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}} \prod_{t=1}^n \\ \sum_{\tilde{x}_{\mathcal{Q}', t} \in \mathcal{X}_{\mathcal{Q}'}} P'_{X_{\mathcal{Q}'}|X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}(\tilde{x}_{\mathcal{Q}', t} | f_{\mathcal{T}, t}(\tilde{m}_{\mathcal{T}}), f_{\mathcal{Q}' \setminus \mathcal{Q}, t}(m_{\mathcal{Q}' \setminus \mathcal{Q}})) \\ W^n(\mathbf{y}_t | \tilde{x}_{\mathcal{Q}', t}, f_{\mathcal{T}, t}(m_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q}')^c, t}(m_{(\mathcal{T} \cup \mathcal{Q}')^c})) \\ \stackrel{(a)}{=} \frac{1}{|\mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}|} \sum_{m_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c} \in \mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}} \prod_{t=1}^n \\ \sum_{x'_{\mathcal{Q}, t} \in \mathcal{X}_{\mathcal{Q}}} P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}(x'_{\mathcal{Q}, t} | f_{\mathcal{T}, t}(m_{\mathcal{T}}), f_{\mathcal{Q} \setminus \mathcal{Q}, t}(m_{\mathcal{Q} \setminus \mathcal{Q}})) \\ W^n(\mathbf{y}_t | x'_{\mathcal{Q}, t}, f_{\mathcal{T}, t}(\tilde{m}_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q})^c, t}(m_{(\mathcal{T} \cup \mathcal{Q})^c})) \\ = \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}, m_{\mathcal{T}}}} [e_{\mathcal{Q}, \mathcal{T}}(\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q}, m_{\mathcal{T}}})], \quad (212)$$

where (a) follows from (209).

Arguing along the lines of [22, (3.29) in page 187],

$$2P_e \geq \frac{1}{|\mathcal{M}_{\mathcal{T}}|} \sum_{\tilde{m}_{\mathcal{T}}} \sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq \tilde{m}_{\mathcal{T}}} \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}}} [e_{\mathcal{Q}, \mathcal{T}}(\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q}})] \\ + \frac{1}{|\mathcal{M}_{\mathcal{T}}|} \sum_{m_{\mathcal{T}}} \sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq m_{\mathcal{T}}} \mathbb{E}_{\tilde{\mathbf{X}}_{\mathcal{Q}'}} [e_{\mathcal{Q}', \mathcal{T}}(\bar{\mathbf{y}}, m_{\mathcal{T}}, \tilde{\mathbf{X}}_{\mathcal{Q}'})]$$

$$\sum_{\mathbf{x}'_{\mathcal{Q}} \in \mathcal{X}_{\mathcal{Q}}^n} \left(\frac{1}{|\mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}|} \sum_{\substack{m_{\mathcal{Q} \setminus \mathcal{Q}'} \\ \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}}} P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}^n(\mathbf{x}'_{\mathcal{Q}} | f_{\mathcal{T}}(m_{\mathcal{T}}), f_{\mathcal{Q} \setminus \mathcal{Q}'}(m_{\mathcal{Q} \setminus \mathcal{Q}'})) \right) \\ = \frac{1}{|\mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}| \times |\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q})^c}|} \sum_{m_{\mathcal{Q} \setminus \mathcal{Q}'} \in \mathcal{M}_{\mathcal{Q} \setminus \mathcal{Q}'}} \sum_{m_{(\mathcal{T} \cup \mathcal{Q})^c} \in \mathcal{M}_{(\mathcal{T} \cup \mathcal{Q})^c}} \prod_{t=1}^n \left(\sum_{\mathbf{x}'_{\mathcal{Q}, t} \in \mathcal{X}_{\mathcal{Q}}} P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}(\mathbf{x}'_{\mathcal{Q}, t} | f_{\mathcal{T}, t}(m_{\mathcal{T}}), f_{\mathcal{Q} \setminus \mathcal{Q}, t}(m_{\mathcal{Q} \setminus \mathcal{Q}})) \right. \\ \left. W(\mathbf{y}_t | \mathbf{x}'_{\mathcal{Q}, t}, f_{\mathcal{T}, t}(\tilde{m}_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q})^c, t}(m_{(\mathcal{T} \cup \mathcal{Q})^c})) \right) \\ = \frac{1}{|\mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}|} \sum_{m_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c} \in \mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}} \prod_{t=1}^n \left(\sum_{\mathbf{x}'_{\mathcal{Q}, t} \in \mathcal{X}_{\mathcal{Q}}} P_{X_{\mathcal{Q}}|X_{\mathcal{T} \cup (\mathcal{Q} \setminus \mathcal{Q}')}}(\mathbf{x}'_{\mathcal{Q}, t} | f_{\mathcal{T}, t}(m_{\mathcal{T}}), f_{\mathcal{Q} \setminus \mathcal{Q}, t}(m_{\mathcal{Q} \setminus \mathcal{Q}})) \right. \\ \left. W(\mathbf{y}_t | \mathbf{x}'_{\mathcal{Q}, t}, f_{\mathcal{T}, t}(\tilde{m}_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q})^c, t}(m_{(\mathcal{T} \cup \mathcal{Q})^c})) \right) \\ = \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}, m_{\mathcal{T}}}} [e_{\mathcal{Q}, \mathcal{T}}(\bar{\mathbf{y}}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q}, m_{\mathcal{T}}})]. \quad (210)$$

$$\begin{aligned}
& \sum_{\tilde{\mathbf{x}}_{\mathcal{Q}'} \in \mathcal{X}_{\mathcal{Q}'}^n} \left(\frac{1}{|\mathcal{M}_{\mathcal{Q}' \setminus \mathcal{Q}}|} \sum_{m_{\mathcal{Q}' \setminus \mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}' \setminus \mathcal{Q}}} P_{X_{\mathcal{Q}'} | X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}^n(\tilde{\mathbf{x}}_{\mathcal{Q}'} | f_{\mathcal{T}}(\tilde{m}_{\mathcal{T}}), f_{\mathcal{Q}' \setminus \mathcal{Q}}(m_{\mathcal{Q}' \setminus \mathcal{Q}})) \right) \\
& \quad \frac{1}{|\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}|} \sum_{m_{(\mathcal{T} \cup \mathcal{Q}')^c} \in \mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}} W^n(\mathbf{y} | \tilde{\mathbf{x}}_{\mathcal{Q}'}, f_{\mathcal{T}}(m_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q}')^c}(m_{(\mathcal{T} \cup \mathcal{Q}')^c})) \\
& = \frac{1}{|\mathcal{M}_{\mathcal{Q}' \setminus \mathcal{Q}}| \times |\mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}|} \sum_{m_{\mathcal{Q}' \setminus \mathcal{Q}} \in \mathcal{M}_{\mathcal{Q}' \setminus \mathcal{Q}}} \sum_{m_{(\mathcal{T} \cup \mathcal{Q}')^c} \in \mathcal{M}_{(\mathcal{T} \cup \mathcal{Q}')^c}} \prod_{t=1}^n \sum_{\tilde{x}_{\mathcal{Q}',t} \in \mathcal{X}_{\mathcal{Q}'}} P'_{X_{\mathcal{Q}'} | X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}(\tilde{x}_{\mathcal{Q}',t} | f_{\mathcal{T},t}(\tilde{m}_{\mathcal{T}}), f_{\mathcal{Q}' \setminus \mathcal{Q},t}(m_{\mathcal{Q}' \setminus \mathcal{Q}})) \\
& \quad W(\mathbf{y}_t | \tilde{x}_{\mathcal{Q}',t}, f_{\mathcal{T},t}(m_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q}')^c,t}(m_{(\mathcal{T} \cup \mathcal{Q}')^c})) \\
& = \frac{1}{|\mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}|} \sum_{m_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c} \in \mathcal{M}_{(\mathcal{T} \cup (\mathcal{Q} \cap \mathcal{Q}'))^c}} \prod_{t=1}^n \sum_{\tilde{x}_{\mathcal{Q}',t} \in \mathcal{X}_{\mathcal{Q}'}} P'_{X_{\mathcal{Q}'} | X_{\mathcal{T} \cup (\mathcal{Q}' \setminus \mathcal{Q})}}(\tilde{x}_{\mathcal{Q}',t} | f_{\mathcal{T},t}(\tilde{m}_{\mathcal{T}}), f_{\mathcal{Q}' \setminus \mathcal{Q},t}(m_{\mathcal{Q}' \setminus \mathcal{Q}})) \\
& \quad W(\mathbf{y}_t | \tilde{x}_{\mathcal{Q}',t}, f_{\mathcal{T},t}(m_{\mathcal{T}}), f_{(\mathcal{T} \cup \mathcal{Q}')^c,t}(m_{(\mathcal{T} \cup \mathcal{Q}')^c})) \\
& = \mathbb{E}_{\tilde{\mathbf{X}}_{\mathcal{Q}',\tilde{m}_{\mathcal{T}}}} \left[e_{\mathcal{Q}',\mathcal{T}}(\mathbf{y}, m_{\mathcal{T}}, \tilde{\mathbf{X}}_{\mathcal{Q}',\tilde{m}_{\mathcal{T}}}) \right]. \tag{211}
\end{aligned}$$

for any attack vectors $\mathbf{X}'_{\mathcal{Q}}$ and $\tilde{\mathbf{X}}_{\mathcal{Q}'}$. In particular, for the attack vectors $\frac{1}{|\mathcal{M}_{\mathcal{T}}|} \sum_{\tilde{m}_{\mathcal{T}}} \tilde{\mathbf{X}}_{\mathcal{Q}',\tilde{m}_{\mathcal{T}}}$ and $\frac{1}{|\mathcal{M}_{\mathcal{T}}|} \sum_{m_{\mathcal{T}}} \mathbf{X}'_{\mathcal{Q},m_{\mathcal{T}}}$,

$$\begin{aligned}
& 2P_e \\
& \geq \frac{1}{|\mathcal{M}_{\mathcal{T}}|^2} \sum_{\tilde{m}_{\mathcal{T}}} \sum_{m_{\mathcal{T}}} \left(\sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq \tilde{m}_{\mathcal{T}}} \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}}} [e_{\mathcal{Q},\mathcal{T}}(\mathbf{y}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q},m_{\mathcal{T}}})] \right. \\
& \quad \left. + \sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq m_{\mathcal{T}}} \mathbb{E}_{\tilde{\mathbf{X}}_{\mathcal{Q}'}} [e_{\mathcal{Q}',\mathcal{T}}(\mathbf{y}, m_{\mathcal{T}}, \tilde{\mathbf{X}}_{\mathcal{Q}',\tilde{m}_{\mathcal{T}}})] \right) \\
& \stackrel{(a)}{=} \frac{1}{|\mathcal{M}_{\mathcal{T}}|^2} \sum_{\tilde{m}_{\mathcal{T}}} \sum_{m_{\mathcal{T}}} \left(\sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq \tilde{m}_{\mathcal{T}}} \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}}} [e_{\mathcal{Q},\mathcal{T}}(\mathbf{y}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q},m_{\mathcal{T}}})] \right. \\
& \quad \left. + \sum_{\mathbf{y}: \phi(\mathbf{y})_{\mathcal{T}} \neq m_{\mathcal{T}}} \mathbb{E}_{\mathbf{X}'_{\mathcal{Q}}} [e_{\mathcal{Q},\mathcal{T}}(\mathbf{y}, \tilde{m}_{\mathcal{T}}, \mathbf{X}'_{\mathcal{Q},m_{\mathcal{T}}})] \right),
\end{aligned}$$

where (a) follows from (212). For $m_{\mathcal{T}} \neq \tilde{m}_{\mathcal{T}}$, the term in brackets on the right is upper bounded by 1, otherwise it is upper bounded by zero. Thus,

$$P_e \geq \frac{|\mathcal{M}_{\mathcal{T}}|(|\mathcal{M}_{\mathcal{T}}| - 1)/2}{2|\mathcal{M}_{\mathcal{T}}|^2} \geq \frac{1}{8}.$$

This completes the proof of the converse. \square

ACKNOWLEDGMENT

The authors would like to thank Sidharth Jaggi, the anonymous reviewers, and the associate editor for their thoughtful comments which helped greatly improve the presentation.

REFERENCES

- [1] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Multiple access channels with Byzantine users," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Aug. 2019, pp. 1–5.
- [2] A. Burg, A. Chattopadhyay, and K.-Y. Lam, "Wireless communication and security issues for cyber-physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018.
- [3] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.
- [4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [5] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Statist.*, vol. 31, no. 3, pp. 558–567, Sep. 1960.
- [6] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2148–2177, Oct. 1998.
- [7] A. Beemer, E. Graves, J. Kliewer, O. Kosut, and P. Yu, "Authentication and partial message correction over adversarial multiple-access channels," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–6.
- [8] J.-H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 2, pp. 212–226, Mar. 1981.
- [9] J. A. Gubner, "On the deterministic-code capacity of the multiple-access arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 36, no. 2, pp. 262–275, Mar. 1990.
- [10] R. Ahlswede and N. Cai, "Arbitrarily varying multiple-access channels. I. Ericson's symmetrization is adequate, Gubner's conjecture is true," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 742–749, Mar. 1999.
- [11] U. Pereg and Y. Steinberg, "The capacity region of the arbitrarily varying MAC: With and without constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 445–449.
- [12] M. Wiese and H. Boche, "The arbitrarily varying multiple-access channel with conferencing encoders," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1405–1416, Mar. 2013.
- [13] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.
- [14] O. Kosut, L. Tong, and D. N. C. Tse, "Polytope codes against adversaries in networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3308–3344, Jun. 2014.
- [15] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, "Resilient network coding in the presence of Byzantine adversaries," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2007, pp. 616–624.
- [16] D. Wang, D. Silva, and F. R. Kschischang, "Robust network coding in the presence of untrusted nodes," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4532–4538, Sep. 2010.
- [17] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.
- [18] R. La and V. Anantharam, "A game-theoretic look at the Gaussian multiaccess channel," *Discrete Math. Theor. Comput. Sci.*, vol. 66, pp. 87–106, Mar. 2004.
- [19] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Multiple access channels with adversarial users," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 435–439.
- [20] N. Sangwan, M. Bakshi, B. K. Dey, and V. M. Prabhakaran, "Communication with adversary identification in Byzantine multiple access channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 688–693.

- [21] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 1, pp. 42–48, Jan. 1985.
- [22] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.
- [23] G. Dueck, "Maximal error capacity regions are smaller than average error capacity regions for multi-user channels," *Problems Control Inf. Theory*, vol. 7, pp. 11–19, 1978. [Online]. Available: <https://pascal-francis.inist.fr/vibad/index.php?action=getRecordDetail&lang=en&idt=PASCAL7930024509>
- [24] S. Janson and A. Ruciński, "The deletion method for upper tail estimates," *Combinatorica*, vol. 24, no. 4, pp. 615–640, Sep. 2004.
- [25] M. Fitzi, M. Hirt, and U. Maurer, "General adversaries in unconditional multi-party computation," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT)*. Singapore: Springer, 1999, pp. 232–246. [Online]. Available: <https://link.springer.com/book/10.1007/b72231>
- [26] M. Hirt and U. Maurer, "Player simulation and general adversary structures in perfect multiparty computation," *J. Cryptol.*, vol. 13, no. 1, pp. 31–60, Jan. 2000.
- [27] T. Wu, S. Zhu, F. Li, and L. Liu, "Two quantum secret sharing schemes with adversary structure," *Int. J. Theor. Phys.*, vol. 61, no. 7, pp. 1–21, Jul. 2022.
- [28] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
- [29] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
- [30] J. A. Gubner and B. L. Hughes, "Nonconvexity of the capacity region of the multiple-access arbitrarily varying channel subject to constraints," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 3–13, Jan. 1995.

Neha Sangwan received the B.E. degree from the Delhi College of Engineering, University of Delhi, in 2013, the M.Sc. degree from the Chennai Mathematical Institute, Chennai, Tamil Nadu, in 2017, and the Ph.D. degree from the Tata Institute of Fundamental Research, Mumbai, in 2023.

Mayank Bakshi (Member, IEEE) received the B.Tech. and M.Tech. degrees from the Indian Institute of Technology Kanpur, India, in 2003 and 2005, respectively, and the Ph.D. degree from the California Institute of Technology in 2011. He was a Post-Doctoral Scholar and a Research Assistant Professor with The Chinese University of Hong Kong, from 2012 to 2019, and a Principal Researcher with the Theory Laboratory, Huawei, Hong Kong, from 2019 to 2021. He is currently a Research Scientist at Arizona State University. His research interests include physical layer security, adversarial robust communications and learning, and sparse recovery.

Bikash Kumar Dey (Member, IEEE) received the M.E. degree in signal processing and the Ph.D. degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, India, in 1999 and 2003, respectively.

In 2003, he joined the International Institute of Information Technology, Hyderabad, India, as an Assistant Professor. In 2005, he joined the Department of Electrical Engineering, Indian Institute of Technology Bombay, as an Assistant Professor, where he is currently a Professor. His research interests include information theory, coding theory, and wireless communications. He was awarded the Prof. I. S. N. Murthy Medal from IISc as the Best M.E. Student with the Department of Electrical Communication Engineering and the Department of Electrical Engineering from 1998 to 1999 and the Alumni Medal for Best Ph.D. Thesis from the Division of Electrical Sciences from 2003 to 2004. He was an Associate Editor of IEEE TRANSACTIONS ON INFORMATION THEORY from 2018 to 2020.

Vinod M. Prabhakaran (Member, IEEE) received the M.E. degree from the Indian Institute of Science in 2001 and the Ph.D. degree from the University of California at Berkeley in 2007. He was a Post-Doctoral Researcher with the University of Illinois at Urbana–Champaign and Ecole Polytechnique Fédérale de Lausanne, Switzerland. Since 2011, he has been with the School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai. His research interests include information theory, cryptography, and communication. He is an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY.