Commitment over Multiple-Access Channels

Rémi Chou* and Matthieu R. Bloch†
*Department of Electrical Engineering & Computer Science, Wichita State University, Wichita, KS 67260, USA
†School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA
Email: {remi.chou@wichita.edu,matthieu.bloch@ece.gatech.edu}

2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton) | 979-8-3503-9998-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ALLERTON49937.2022.9929405

***Abstract*—The problem of multi-user commitment is one in which multiple users first commit to individual messages with a bookmaker and later reveal their messages. The objective of the bookmaker is then to decide whether the revealed messages correspond to the committed messages. We study a specific multi-user commitment model in which the users and the bookmaker have access to a noiseless channel, as well as a noisy multiple-access channel whose inputs are controlled by the users and whose output is observed by the bookmaker. When the users are non-colluding and the channel is non-redundant, we fully characterize the commitment capacity region. When the users are colluding, we derive an achievable region and a tight converse for the sum-rate. In both cases our proposed achievable commitment schemes are constructive.**

I. Introduction

Commitment without the need for a trusted third party can be traced back to Blum's coin flipping problem [1]. More generally, a two-party commitment problem involves a sender, Alice, and a receiver, Bob, and operates in two phases. In the first phase, called the commit phase, Alice sends information to Bob to commit to a message M that must be concealed from Bob. In the second phase, called the reveal phase, Alice reveals a message M' to Bob, who must determine whether M' is the message that Alice committed to in the commit phase. Additionally, the protocol must be binding in the sense that, in the reveal phase, Alice cannot make Bob believe that she committed to a message $M' \neq M$. It is well-known that information-theoretic concealment guarantees cannot be achieved over noiseless communication channels. However, when a noisy channel is available as resource, both concealment and binding requirements can be obtained under information-theoretic guarantees, i.e., when Alice and Bob are not assumed to be computationally limited, for some class noisy channels called non-redundant [2].

While most of the literature focuses on two-party commitment, e.g., [2]–[9], we study here multi-user commitment. Specifically, we consider a commitment setting between a bookmaker and L users who want to commit to individual messages. To this end, the L users and the bookmaker have access to a noiseless public communication channel and a noisy discrete memoryless multiple-access channel with L inputs. Each input of the multiple-access channel is controlled by a distinct user and the bookmaker observes the output of the channel. Similar to a two-party setting, the protocol consists of a commit phase and a reveal phase. Here, the concealment requirement is that the bookmaker must not learn, in an information-theoretic sense, information about any message of any user after the commit phase. The protocol must also be information-theoretically binding in the sense that, during the reveal phase, a user cannot make the bookmaker believe that it committed to another message than the one committed to in the commit phase. In this study, we consider both the cases of colluding and non-colluding users. The non-colluding users case corresponds to a scenario in which the users do not trust each other and do not want to exchange information with one another. For instance, this would be the case when the users are bidders that commit to messages sent to an auctioneer. Under a non-redundancy condition on the multiple-access channel, we derive the capacity region for the non-colluding users case, and an achievable region and the sum-rate capacity for the colluding users case. In both cases, our achievability scheme is constructive and relies on distributing hashing with two-universal hash functions [10] for the concealment guarantees. The bindingness of our achievability scheme hinges on the non-redundancy property of the multiple access channel akin to the two-party commitment in [2]. The characterization of the sum-rate capacity relies on the polymatroidal properties of our achievability region.

The remainder of the paper is organized as follows. We formally state the problem in Section II. We describe our main results in Section III. Our achievability scheme and its analysis are presented in Sections IV and V, respectively. Finally, our converse result is presented in Section VI.

II. Problem Statement

Let $L \in \mathbb{N}^*$ and define $\mathcal{L} \triangleq [\![1, L]\!]$. Let $(\mathcal{X}_l)_{l\in\mathcal{L}}$ and $\mathcal{Y}$ be finite alphabets and define the cartesian product $\mathcal{X}_{\mathcal{L}} \triangleq \bigtimes_{l\in\mathcal{L}} \mathcal{X}_l$. Consider a multiple access channel $W \triangleq (\mathcal{Y}, p_{Y|X_{\mathcal{L}}}, \mathcal{X}_{\mathcal{L}})$, where $X_{\mathcal{L}} \triangleq (X_l)_{l\in\mathcal{L}}$ and X_l, $l \in \mathcal{L}$, is defined over $\mathcal{X}_l$. For any $x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}$, define $W_{x_{\mathcal{L}}} : y \mapsto p_{Y|X_{\mathcal{L}}}(y|x_{\mathcal{L}})$. Let $\mathcal{P}(\mathcal{X}_{\mathcal{L}})$ be the set of probability distribution over $\mathcal{X}_{\mathcal{L}}$. We assume that throughout the multiple access channel W is non-redundant as defined in [2], i.e.,

$$\forall x_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}, \forall p_{X_{\mathcal{L}}} \in \mathcal{P}(\mathcal{X}_{\mathcal{L}}) \text{ s.t. } p_{X_{\mathcal{L}}}(x_{\mathcal{L}}) = 0, \quad W_{x_{\mathcal{L}}} \neq \sum_{x'_{\mathcal{L}} \in \mathcal{X}_{\mathcal{L}}} p_{X_{\mathcal{L}}}(x'_{\mathcal{L}}) W_{x'_{\mathcal{L}}}. \quad (1)$$

Next, we introduce two models of commitment. In Model 1 the transmitters are colluding, while in Model 2 they are not.

This work was supported in part by NSF grant CCF-2047913.

A. Model 1: Colluding transmitters

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

- *For every $l \in \mathcal{L}$, a sequence $a_l \in \mathcal{A}_l \triangleq [\![1, 2^{nR_l}]\!]$ that Transmitter $l \in \mathcal{L}$ wishes to commit to;*
- *A public noiseless communication channel between the transmitters and the receiver;*
- *Local randomness $S \in \mathcal{R}$ available at the transmitters;*
- *Local randomness $S' \in \mathcal{R}'$ available at the receiver and used in the interactive noiseless communication with all L transmitters during the commit phase;*

and operates in two phases as follows.

1) *Commit phase: Define $a_{\mathcal{L}} \triangleq (a_l)_{l\in\mathcal{L}}$. For channel use $i \in [\![1, n]\!]$, the transmitters send $X_{\mathcal{L},i}(a_{\mathcal{L}}, S, M'_{1:i-1,r_{i-1}})$ over the channel and engage in r_i rounds of noiseless public communication with the receiver, i.e., for $j \in [\![1, r_i]\!]$, the transmitters send $M_{i,j}(a_{\mathcal{L}}, S, M'_{1:i,1:j-1})$ and the receiver replies $M'_{i,j}(S', M_{1:i,1:j}, Y^i)$. We denote the collective noiseless communication between the transmitters and the receiver by M. Define $V \triangleq (Y^n, M, S')$.*
2) *Reveal phase: Transmitters reveal $(a_{\mathcal{L}}, S)$. The receiver performs a test $\beta(V, a_{\mathcal{L}}, S)$ that returns 1 if the sequence $a_{\mathcal{L}}$ is accepted and 0 otherwise.*

Definition 2. *A rate-tuple $(R_l)_{l\in\mathcal{L}}$ is achievable if there exists a sequence of $((2^{nR_l})_{l\in\mathcal{L}}, n)$ commitment schemes such that for any $\tilde{S} \in \mathcal{R}$, $a_{\mathcal{L}}, a'_{\mathcal{L}} \in \mathcal{A}_{\mathcal{L}}$ such that $a_{\mathcal{L}} \neq a'_{\mathcal{L}}$,*

$$\lim_{n\to\infty} \mathbb{P}[\beta(V, a_{\mathcal{L}}, S) = 0] = 0, \text{ (correctness)}$$

$$\lim_{n\to\infty} I(A_{\mathcal{L}}; V) = 0, \text{ (concealment)}$$

$$\lim_{n\to\infty} \mathbb{P}[\beta(V, a_{\mathcal{L}}, S) = 1 = \beta(V, a'_{\mathcal{L}}, \tilde{S})] = 0. \text{ (bindingness)}$$

The set of all achievable rate-tuples is the capacity region.

B. Model 2: Non-colluding transmitters

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

- *For every $l \in \mathcal{L}$, a sequence $a_l \in \mathcal{A}_l \triangleq [\![1, 2^{nR_l}]\!]$ that Transmitter $l \in \mathcal{L}$ wants to commit to;*
- *A noiseless private channel between each transmitter and the receiver;*
- *Local randomness $S_l \in \mathcal{R}_l$ at Transmitter $l \in \mathcal{L}$;*
- *Local randomness $S'_l \in \mathcal{R}'_l$, $l \in \mathcal{L}$, at the receiver where S'_l is only used in the interactive noiseless communication with Transmitter $l \in \mathcal{L}$ during the commit phase;*

and operates in two phases as follows.

1) *Commit phase: For each $l \in \mathcal{L}$, for $i \in [\![1, n]\!]$, Transmitter l sends $X_{l,i}(a_l, S_l, M'_{l,1:i-1,r_{i-1}})$ over the channel and engage in r_i rounds of noiseless public communication with the receiver, i.e., for $j \in [\![1, r_i]\!]$, Transmitter l sends $M_{l,i,j}(a_l, S_l, M'_{l,1:i,1:j-1})$ and the receiver replies $M'_{l,i,j}(S'_l, M_{l,1:i,1:j}, Y^i)$. We denote the collective noiseless public communication between Transmitter $l \in \mathcal{L}$ and the receiver by M_l. Define $V_l \triangleq (Y^n, M_l, S'_l)$ for $l \in \mathcal{L}$ and $V_{\mathcal{L}} \triangleq (V_l)_{l\in\mathcal{L}}$, $a_{\mathcal{L}} \triangleq (a_l)_{l\in\mathcal{L}}$.*
2) *Reveal phase: Transmitter $l \in \mathcal{L}$ reveals (a_l, S_l). For each $l \in \mathcal{L}$, the receiver performs a test $\beta_l(V_l, a_l, S_l)$, $l \in \mathcal{L}$, that return 1 if the sequence a_l is accepted and 0 otherwise.*

Definition 4. *A rate-tuple $(R_l)_{l\in\mathcal{L}}$ is achievable if there exists a sequence of $((2^{nR_l})_{l\in\mathcal{L}}, n)$ commitment schemes such that for any $l \in \mathcal{L}$, $\tilde{S}_l \in \mathcal{R}_l$, $a_{\mathcal{L}}, a'_{\mathcal{L}} \in \mathcal{A}_{\mathcal{L}}$ such that $a_{\mathcal{L}} \neq a'_{\mathcal{L}}$,*

$$\lim_{n\to\infty} \mathbb{P}[\beta_l(V_l, a_l, S_l) = 0] = 0, \text{ (correctness)}$$

$$\lim_{n\to\infty} I(A_{\mathcal{L}}; V_{\mathcal{L}}) = 0, \text{ (concealment)}$$

$$\lim_{n\to\infty} \mathbb{P}[\beta_l(V_l, a_l, S_l) = 1 = \beta_l(V_l, a'_l, \tilde{S}_l)] = 0. \text{ (bindingness)}$$

The set of all achievable rate-tuples is the capacity region.

Note that since V depends on Y^n, which depends on all user inputs to the channel, $I(A_{\mathcal{L}}; V_{\mathcal{L}}) \neq \sum_{l\in\mathcal{L}} I(A_l; V_l)$.

III. Main results

Our main results are a partial characterization of the capacity region in the case of colluding transmitters (Theorem 1) and a complete characterization of the capacity region in the case of non-colluding transmitters (Theorem 2). In the following, for any $\mathcal{T} \subseteq \mathcal{L}$, we write the sum-rate of the transmitters in $\mathcal{T}$ as $R_{\mathcal{T}} \triangleq \sum_{l\in\mathcal{T}} R_l$.

Theorem 1. *For the case of colluding transmitters,*

- *The following region is achievable*

$$\bigcup_{p_{X_{\mathcal{L}}} \in \mathcal{P}(\mathcal{X}_{\mathcal{L}})} \{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{T}} \leqslant H(X_{\mathcal{T}}|Y), \forall \mathcal{T} \subseteq \mathcal{L}\}.$$

- *The sum-rate capacity is*

$$\max_{p_{X_{\mathcal{L}}} \in \mathcal{P}(\mathcal{X}_{\mathcal{L}})} H(X_{\mathcal{L}}|Y).$$

Theorem 2. *Define the set of product input distributions*

$$\mathcal{P}^{\mathrm{I}}(\mathcal{X}_{\mathcal{L}}) \triangleq \{p_{X_{\mathcal{L}}} \in \mathcal{P}(\mathcal{X}_{\mathcal{L}}) : p_{X_{\mathcal{L}}} = \prod_{l\in\mathcal{L}} p_{X_l}\}.$$

For the case of non-colluding transmitters,

- *The capacity region is*

$$\bigcup_{p_{X_{\mathcal{L}}} \in \mathcal{P}^{\mathrm{I}}(\mathcal{X}_{\mathcal{L}})} \{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{T}} \leqslant H(X_{\mathcal{T}}|Y), \forall \mathcal{T} \subseteq \mathcal{L}\}.$$

- *The sum-rate capacity is*

$$\max_{p_{X_{\mathcal{L}}} \in \mathcal{P}^{\mathrm{I}}(\mathcal{X}_{\mathcal{L}})} H(X_{\mathcal{L}}|Y).$$

The proof of the theorems are developed in the next sections.

IV. Achievability scheme for Theorems 1 and 2

The achievability proofs for the two theorems are similar, differing only in the set of allowed input distributions to the channel. To simultaneously capture both proofs, we define

$$\bar{\mathcal{P}}(\mathcal{X}_{\mathcal{L}}) \triangleq \begin{cases} \mathcal{P}^{\mathrm{I}}(\mathcal{X}_{\mathcal{L}}) & \text{if the transmitters are non-colluding} \\ \mathcal{P}(\mathcal{X}_{\mathcal{L}}) & \text{if the transmitters are colluding} \end{cases}.$$

Fix $p_{X_{\mathcal{L}}} \in \bar{\mathcal{P}}(\mathcal{X}_{\mathcal{L}})$. Define $q_{X_{\mathcal{L}}Y} \triangleq p_{X_{\mathcal{L}}} p_{Y|X_{\mathcal{L}}}$. Consider $X_{\mathcal{L}}^n$ distributed according to $p_{X_{\mathcal{L}}}^{\otimes n}$.

Commit Phase: Transmitter $l \in \mathcal{L}$ commits to a_l as follows.

- Transmitter l sends the sequence X_l^n over the multiple access channel W. The receiver observes Y^n.
- The receiver chooses a function $G_l : \mathcal{X}_l \to \{0,1\}^{\eta n}$ at random in a family of two-universal hash functions with $\eta > 0$, and sends G_l to Transmitter l over the noiseless channel.
- Transmitter l sends $G_l(X_l^n)$ to the receiver over the noiseless channel. Let T_l be the corresponding sequence observed by the receiver.
- Transmitter l chooses a function $F_l : \mathcal{X}_l \to \{0,1\}^{r_l}$ at random in a family of two-universal hash functions, and sends F_l and $E_l \triangleq a_l \oplus F_l(\bar{X}_l^n)$ over the noiseless channel, where $\bar{X}_l^n \triangleq X_l^n[(\bigcup_{l \in \mathcal{L}} \mathcal{S}_l)^c]$.

Reveal Phase: Transmitter $l \in \mathcal{L}$ reveals a_l as follows.

- Transmitter l sends X_l^n and a_l to the receiver over the noiseless channel.
- The receiver tests that

(i) $(X_{\mathcal{L}}^n, Y^n) \in \mathcal{T}_\epsilon^n(q_{X_{\mathcal{L}}Y})$;
(ii) $T_l = G_l(X_l^n), \forall l \in \mathcal{L}$;
(iii) $a_l = E_l \oplus F_l(\bar{X}_l^n), \forall l \in \mathcal{L}$;

and outputs 1 if all conditions are satisfied, and 0 else.

V. Analysis of the Achievability Scheme

A. Definitions

The following notions of typicality will prove useful in the proof. Let $\epsilon > 0$. For $x_{\mathcal{L}}^n \in \mathcal{X}_{\mathcal{L}}^n$, define

$$\mathcal{T}_{W,\epsilon}^n(x_{\mathcal{L}}^n) \triangleq \{y^n \in \mathcal{Y}^n : \forall x_{\mathcal{L}}, \forall y,$$
$$\left| \sum_{t=1}^n \frac{\mathbb{1}\{(x_{\mathcal{L}}, y) = (x_{\mathcal{L},t}, y_t)\}}{n} - W_{x_{\mathcal{L}}}(y) \sum_{t=1}^n \frac{\mathbb{1}\{x_{\mathcal{L}} = x_{\mathcal{L},t}\}}{n} \right| \leqslant \epsilon$$
$$\text{and } W_{x_{\mathcal{L}}}(y) = 0 \implies \sum_{t=1}^n \frac{\mathbb{1}\{(x_{\mathcal{L}}, y) = (x_{\mathcal{L},t}, y_t)\}}{n} = 0 \Bigg\}.$$

Define also

$$\mathcal{T}_\epsilon^n(q_{X_{\mathcal{L}}Y}) \triangleq \{(x_{\mathcal{L}}^n, y^n) \in \mathcal{X}_{\mathcal{L}}^n \times \mathcal{Y}^n : \forall x_{\mathcal{L}}, \forall y,$$
$$\left| \sum_{t=1}^n \frac{\mathbb{1}\{(x_{\mathcal{L}}, y) = (x_{\mathcal{L},t}, y_t)\}}{n} - q_{X_{\mathcal{L}}Y}(x_{\mathcal{L}}, y) \right| \leqslant \epsilon \text{ and}$$
$$q_{X_{\mathcal{L}}Y}(x_{\mathcal{L}}, y) = 0 \implies \sum_{t=1}^n \frac{\mathbb{1}\{(x_{\mathcal{L}}, y) = (x_{\mathcal{L},t}, y_t)\}}{n} = 0 \Bigg\}.$$

B. Correctness

When the parties are not cheating, standard typicality arguments [11] show that $\lim_{n\to\infty} \mathbb{P}[(X_{\mathcal{L}}^n, Y^n) \in \mathcal{T}_\epsilon^n(q_{X_{\mathcal{L}}Y})] = 1$. Consequently, part (i) of the receiver test passes, while part (ii) and (iii) are automatically true, so that the receiver estimates $a_{\mathcal{L}}$ with vanishing probability of error in the reveal phase.

C. Concealment

Define $V' \triangleq (\mathcal{S}_{\mathcal{L}}, F_{\mathcal{L}}, X_{\mathcal{L}}^n[\mathcal{S}_{\mathcal{L}}], Y^n)$ and $V \triangleq (V', E_{\mathcal{L}})$, where $\mathcal{S}_{\mathcal{L}} \triangleq (\mathcal{S}_l)_{l \in \mathcal{L}}$, $F_{\mathcal{L}} \triangleq (F_l)_{l \in \mathcal{L}}$, $E_{\mathcal{L}} \triangleq (E_l)_{l \in \mathcal{L}}$, $X_{\mathcal{L}}^n[\mathcal{S}_{\mathcal{L}}] \triangleq (X_l^n[\mathcal{S}_l])_{l \in \mathcal{L}}$. Note that V captures all the information available to the receiver at the end of the reveal phase. Also define $K_{\mathcal{L}} \triangleq (F_l(X_l^n))_{l \in \mathcal{L}}$ and $Y^n \triangleq Y^n[(\bigcup_{l \in \mathcal{L}} \mathcal{S}_l)^c]$, which represent the sequence of hashes used to protect the committed strings by the transmitters and the channel observations potentially leaking information to the receiver about the hashes, respectively. Then, we have

$$\begin{aligned}
&I(A_{\mathcal{L}}; V) \\
&\overset{(a)}{=} I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(A_{\mathcal{L}}; V'|E_{\mathcal{L}}) \\
&\leqslant I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(A_{\mathcal{L}} E_{\mathcal{L}}; V') \\
&\overset{(b)}{=} I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(A_{\mathcal{L}} K_{\mathcal{L}}; V') \\
&= I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(K_{\mathcal{L}}; V') + I(A_{\mathcal{L}}; V'|K_{\mathcal{L}}) \\
&\leqslant I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(K_{\mathcal{L}}; V') + I(A_{\mathcal{L}}; V' K_{\mathcal{L}}) \\
&\overset{(c)}{=} I(A_{\mathcal{L}}; E_{\mathcal{L}}) + I(K_{\mathcal{L}}; V') \\
&\overset{(d)}{\leqslant} r_{\mathcal{L}} - H(E_{\mathcal{L}}|A_{\mathcal{L}}) + I(K_{\mathcal{L}}; V') \\
&\overset{(e)}{=} r_{\mathcal{L}} - H(K_{\mathcal{L}}) + I(K_{\mathcal{L}}; V') \\
&= r_{\mathcal{L}} - H(K_{\mathcal{L}}) + I(K_{\mathcal{L}}; F_{\mathcal{L}} \bar{Y}^n) \\
&\quad + I(K_{\mathcal{L}}; \mathcal{S}_{\mathcal{L}} X_{\mathcal{L}}^n[\mathcal{S}_{\mathcal{L}}] Y^n[\textstyle\bigcup_{l \in \mathcal{L}} \mathcal{S}_l] | F_{\mathcal{L}} \bar{Y}^n) \\
&\leqslant r_{\mathcal{L}} - H(K_{\mathcal{L}}) + I(K_{\mathcal{L}}; F_{\mathcal{L}} \bar{Y}^n) \\
&\quad + I(F_{\mathcal{L}} \bar{Y}^n K_{\mathcal{L}}; \mathcal{S}_{\mathcal{L}} X_{\mathcal{L}}^n[\mathcal{S}_{\mathcal{L}}] Y^n[\textstyle\bigcup_{l \in \mathcal{L}} \mathcal{S}_l]) \\
&\overset{(f)}{=} r_{\mathcal{L}} - H(K_{\mathcal{L}}) + I(K_{\mathcal{L}}; F_{\mathcal{L}} \bar{Y}^n), \qquad (2)
\end{aligned}$$

where (a) holds by the chain rule and the definition of V, (b) holds by the one-time pad lemma, (c) holds by independence between $A_{\mathcal{L}}$ and $(V', K_{\mathcal{L}})$, (d) holds with $r_{\mathcal{L}} \triangleq \sum_{l \in \mathcal{L}} r_l$, (e) holds by the definition of $E_{\mathcal{L}}$, (f) holds by independence between $(F_{\mathcal{L}}, \bar{Y}^n, K_{\mathcal{L}})$ and $(\mathcal{S}_{\mathcal{L}}, X_{\mathcal{L}}^n[\mathcal{S}_{\mathcal{L}}], Y^n[\bigcup_{l \in \mathcal{L}} \mathcal{S}_l])$. Next, we upper bound the right hand side of (2) using the version of the leftover hash lemma in Lemma 1, and we lower bound the entropies appearing in Lemma 1 using Lemma 2.

Lemma 1 (Distributed leftover hash lemma, e.g., [12, Lemma 1]). *Consider a sub-normalized non-negative function $p_{X_{\mathcal{L}}Z}$ defined over $\bigtimes_{l \in \mathcal{L}} \mathcal{X}_l \times \mathcal{Z}$, where $X_{\mathcal{L}} \triangleq (X_l)_{l \in \mathcal{L}}$ and, $\mathcal{Z}$, $\mathcal{X}_l$, $l \in \mathcal{L}$, are finite alphabets. For $l \in \mathcal{L}$, let $F_l : \{0,1\}^{n_l} \longrightarrow \{0,1\}^{r_l}$, be uniformly chosen in a family $\mathcal{F}_l$ of two-universal hash functions. For any $\mathcal{T} \subseteq \mathcal{L}$, define $r_{\mathcal{T}} \triangleq \sum_{l \in \mathcal{T}} r_l$. Define also $F_{\mathcal{L}} \triangleq (F_l)_{l \in \mathcal{L}}$ and $F_{\mathcal{L}}(X_{\mathcal{L}}) \triangleq (F_l(X_l))_{l \in \mathcal{L}}$. Then, for any q_Z defined over $\mathcal{Z}$ such that* $\mathrm{supp}(q_Z) \subseteq \mathrm{supp}(p_Z)$, *we have*

$$\mathbb{V}(p_{F_{\mathcal{L}}(X_{\mathcal{L}}) F_{\mathcal{L}} Z}, p_{U_{\mathcal{K}}} p_{U_{\mathcal{F}}} p_Z) \leqslant \sqrt{\sum_{\mathcal{T} \subseteq \mathcal{L}, \mathcal{T} \neq \emptyset} 2^{r_{\mathcal{T}} - H_\infty(p_{X_{\mathcal{T}} Z}|q_Z)}}, \qquad (3)$$

where $p_{U_{\mathcal{K}}}$ and $p_{U_{\mathcal{F}}}$ are the uniform distributions over $[\![1, 2^{r_{\mathcal{L}}}]\!]$ and $[\![1, \prod_{l \in \mathcal{L}} |\mathcal{F}_l|]\!]$, respectively, and for any $\mathcal{T} \subseteq \mathcal{L}, \mathcal{T} \neq \emptyset$,

$$H_\infty(p_{X_{\mathcal{T}} Z}|q_Z) \triangleq -\log \max_{\substack{x_{\mathcal{T}} \in \mathcal{X}_{\mathcal{T}} \\ z^n \in \mathrm{supp}(q_Z)}} \frac{p_{X_{\mathcal{T}} Z}(x_{\mathcal{T}}, z)}{q_Z(z)}.$$

Lemma 2 ([12, Lemma 2]). *Let $(\mathcal{X}_l)_{l\in\mathcal{L}}$ be L finite alphabets and define for $\mathcal{T}\subseteq\mathcal{L}$, $\mathcal{X}_\mathcal{T}\triangleq\bigtimes_{l\in\mathcal{T}}\mathcal{X}_d$. Consider the random variables $X_\mathcal{L}^n\triangleq(X_l^n)_{l\in\mathcal{L}}$ and Z^n defined over $\mathcal{X}_\mathcal{L}^n\times\mathcal{Z}^n$ with probability distribution $q_{X_\mathcal{L}^nZ^n}\triangleq\prod_{i=1}^n q_{X_\mathcal{L}Z}$. For any $\epsilon>0$, there exists a subnormalized non-negative function $w_{X_\mathcal{L}^nZ^n}$ defined over $\mathcal{X}_\mathcal{L}^n\times\mathcal{Z}^n$ such that $\mathbb{V}(q_{X_\mathcal{L}^nZ^n},w_{X_\mathcal{L}^nZ^n})\leqslant\epsilon$ and*

$$\forall\mathcal{T}\subseteq\mathcal{L}, H_\infty(w_{X_\mathcal{T}^nZ^n}|q_{Z^n})\geqslant nH(X_\mathcal{T}|Z)-n\delta_\mathcal{T}(n),$$

where $\delta_\mathcal{T}(n)\triangleq(\log(|\mathcal{X}_\mathcal{T}|+3))\sqrt{\frac{2}{n}(L+\log(\frac{1}{\epsilon}))}$.

Let $\epsilon>0$ and define $\bar{n}\triangleq n-|\bigcup_{l\in\mathcal{L}}\mathcal{S}_l|$. By Lemma 2, there exists a subnormalized non-negative function $w_{X_\mathcal{L}^nY^n}$ such that $\mathbb{V}(q_{X_\mathcal{L}^nY^n},w_{X_\mathcal{L}^nY^n})\leqslant\epsilon$ and

$$\forall\mathcal{T}\subseteq\mathcal{L}, H_\infty(w_{\bar{X}_\mathcal{T}^n\bar{Y}^n}|q_{\bar{Y}^n})\geqslant\bar{n}H(X_\mathcal{T}|Y)-\bar{n}\delta_\mathcal{T}(\bar{n}), \quad (4)$$

where $\delta_\mathcal{T}(\bar{n})\triangleq(\log(|\mathcal{X}_\mathcal{T}|+3))\sqrt{\frac{2}{\bar{n}}(L+\log(\frac{1}{\epsilon}))}$. Then, we have by Lemma 1

$$\begin{aligned}
&\mathbb{V}(q_{K_\mathcal{L}F_\mathcal{L}Y^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}q_{Y^n})\\
&\overset{(a)}{\leqslant}\mathbb{V}(q_{K_\mathcal{L}F_\mathcal{L}Y^n},w_{K_\mathcal{L}F_\mathcal{L}Y^n})+\mathbb{V}(w_{K_\mathcal{L}F_\mathcal{L}Y^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}q_{Y^n})\\
&\overset{(b)}{\leqslant}\epsilon+\mathbb{V}(w_{K_\mathcal{L}F_\mathcal{L}\bar{Y}^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}q_{\bar{Y}^n})\\
&\overset{(c)}{\leqslant}\epsilon+\mathbb{V}(w_{K_\mathcal{L}F_\mathcal{L}Y^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}w_{Y^n})\\
&\quad+\mathbb{V}(p_{U_\mathcal{K}}p_{U_\mathcal{F}}w_{\bar{Y}^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}q_{\bar{Y}^n})\\
&\overset{(d)}{\leqslant}2\epsilon+\mathbb{V}(w_{K_\mathcal{L}F_\mathcal{L}Y^n},p_{U_\mathcal{K}}p_{U_\mathcal{F}}w_{Y^n})\\
&\overset{(e)}{\leqslant}2\epsilon+\sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset}2^{r_\mathcal{S}-H_\infty(w_{\bar{X}_\mathcal{T}^n\bar{Y}^n}|q_{\bar{Y}^n})}}\\
&\overset{(f)}{\leqslant}2\epsilon+\sqrt{\sum_{\mathcal{S}\subseteq\mathcal{L},\mathcal{S}\neq\emptyset}2^{r_\mathcal{S}-nH(X_\mathcal{T}|Y)+n\delta_\mathcal{T}(n)}},
\end{aligned}$$

where (a) and (c) hold by the triangle inequality, (b) and (d) hold by the data processing inequality and because $\mathbb{V}(q_{X_\mathcal{L}^nY^n},w_{X_\mathcal{L}^nY^n})\leqslant\epsilon$, (e) holds by Lemma 1, (f) holds by (4). We conclude that concealment holds with $(r_l)_{l\in\mathcal{L}}$ such that for any $\mathcal{T}\subseteq\mathcal{L}$, $\lim_{n\to\infty}\frac{r_\mathcal{T}}{n}\leqslant H(X_\mathcal{T}|Y)$.

D. Achievable region and sum-rate

For any $p_{X_\mathcal{L}}\in\bar{\mathcal{P}}(\mathcal{X}_\mathcal{L})$, we have shown the achievability of

$$\mathcal{R}(p_{X_\mathcal{L}})\triangleq\{(R_l)_{l\in\mathcal{L}}: R_\mathcal{T}\leqslant H(X_\mathcal{T}|Y),\forall\mathcal{T}\subseteq\mathcal{L}\}.$$

Next, define the set function

$$\begin{aligned}f_{p_{X_\mathcal{L}}}:2^\mathcal{L}&\to\mathbb{R}\\ \mathcal{T}&\mapsto H(X_\mathcal{T}|Y).\end{aligned}$$

$f_{p_{X_\mathcal{L}}}$ is normalized, non-decreasing, and submodular because for $\mathcal{U},\mathcal{V}\subseteq\mathcal{L}$, we have

$$\begin{aligned}
&f_{p_{X_\mathcal{L}}}(\mathcal{U}\cup\mathcal{V})+f_{p_{X_\mathcal{L}}}(\mathcal{U}\cap\mathcal{V})\\
&=H(X_\mathcal{U}|Y)+H(X_{\mathcal{V}\setminus\mathcal{U}}|YX_\mathcal{U})+H(X_{\mathcal{U}\cap\mathcal{V}}|Y)\\
&=H(X_\mathcal{U}|Y)+H(X_{\mathcal{V}\setminus\mathcal{U}}|YX_\mathcal{U})+H(X_\mathcal{V}|Y)\\
&\quad-H(X_{\mathcal{V}\setminus\mathcal{U}}|YX_{\mathcal{U}\cap\mathcal{V}})\\
&\leqslant H(X_\mathcal{U}|Y)+H(X_\mathcal{V}|Y)\\
&=f_{p_{X_\mathcal{L}}}(\mathcal{U})+f_{p_{X_\mathcal{L}}}(\mathcal{V}),
\end{aligned}$$

where the inequality holds because conditioning reduces entropy. Hence, by [13], the rate-tuple $(f_{p_{X_\mathcal{L}}}([\![l,L]\!])-f_{p_{X_\mathcal{L}}}([\![l+1,L]\!]))_{l\in\mathcal{L}}$ is achievable and so is the sum-rate

$$R_\mathcal{L}=\max_{p_{X_\mathcal{L}}\in\bar{\mathcal{P}}(\mathcal{X}_\mathcal{L})}H(X_\mathcal{L}|Y).$$

E. Bindingness

We will use the following lemma.

Lemma 3 (Adapted from [2]). *Let $\delta,\sigma>0$. Consider $x_\mathcal{L}^n,\tilde{x}_\mathcal{L}^n\in\mathcal{X}_\mathcal{L}^n$ such that $d_H(x_\mathcal{L}^n,\tilde{x}_\mathcal{L}^n)\geqslant\sigma n$ and a non-redundant multiple access channel W such that for any $b_\mathcal{L}\in\mathcal{X}_\mathcal{L}$,*

$$\forall p_{X_\mathcal{L}}\in\mathcal{P}(\mathcal{X}_\mathcal{L})\ s.t.\ p_{X_\mathcal{L}}(b_\mathcal{L})=0,\quad\mathbb{V}\left(W_{b_\mathcal{L}},\sum_{x_\mathcal{L}\in\mathcal{X}_\mathcal{L}}p_{X_\mathcal{L}}(x_\mathcal{L})W_{x_\mathcal{L}}\right)\geqslant\delta. \quad (5)$$

Then,

$$\lim_{n\to\infty}W_{x_\mathcal{L}^n}^{\otimes n}(\mathcal{T}_{W,\epsilon}^n(\tilde{x}_\mathcal{L}^n))=0.$$

In the reveal phase, if the receiver observes $\tilde{x}_\mathcal{L}^n$, then, by Lemma 3, a successful joint typicality test at the receiver requires $d_H(\tilde{x}_\mathcal{L}^n,x_\mathcal{L}^n)\leqslant O(n^\alpha)$, for some $\alpha<1$. This implies that Test (ii) at the receiver in the reveal phase can only succeed with a probability at most $2^{O(n^\alpha)}2^{-n\eta}$, which vanishes to zero as $n\to\infty$.

VI. Converse for Theorems 1 and 2

We only prove the converse of Theorem 2. The proof, in particular Lemma 5, relies on ideas developed in [2], [9]. The converse proof for the sum-rate in Theorem 1 is similar. Note that we do not obtain a full characterization of the capacity region for the case of colluding users because Lemma 4 below only holds for the case of non-colluding users.

Lemma 4. *Consider the non-colluding transmitters case. For $l\in\mathcal{L}$, $(A_l,S_l)-(M_l,X_l^n)-(Y^n,S_l')$ forms a Markov chain.*

Proof. For $l\in\mathcal{L}$, $i\in[\![1,n]\!]$, $j\in[\![1,r_i]\!]$, define $\bar{M}_{l,1:i,1:j}\triangleq(M_{l,1:i,1:j},M'_{l,1:i,1:j})$ and $\bar{M}_{l,1:i}\triangleq\bar{M}_{l,1:i,1:r_i}$. We have

$$\begin{aligned}
&I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n}X_l^n) \quad (6)\\
&=I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n}X_l^n)\\
&=I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n-1}M_{l,n,r_n}M'_{l,n,r_n}X_l^n)\\
&\leqslant I(A_lS_l;Y^nS_l'M'_{l,n,r_n}|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n-1}M_{l,n,r_n}X_l^n)\\
&\overset{(a)}{=}I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n-1}M_{l,n,r_n}X_l^n)\\
&\leqslant I(A_lS_lM_{l,n,r_n};Y^nS_l'|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n-1}X_l^n)\\
&\overset{(b)}{=}I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n-1}\bar{M}_{l,n,1:r_n-1}X_l^n) \quad (7)\\
&\overset{(c)}{\leqslant}I(A_lS_l;Y^nS_l'|\bar{M}_{l,1:n-1}X_l^n)
\end{aligned}$$

$$
\begin{aligned}
&\overset{(d)}{=} I(A_l S_l; Y^{n-1} S_l' | \bar{M}_{l,1:n-1} X_l^n) \\
&\leqslant I(A_l S_l (X_l)_n; Y^{n-1} S_l' | \bar{M}_{l,1:n-1} X_l^{n-1}) \\
&\overset{(e)}{=} I(A_l S_l; Y^{n-1} S_l' | \bar{M}_{l,1:n-1} X_l^{n-1}) \qquad (8) \\
&\overset{(f)}{\leqslant} I(A_l S_l; S_l') \\
&= 0,
\end{aligned}
$$

where (a) holds because M'_{l,n,r_n} is a function of $(S_l', M_{l,1:n,1:r_n}, Y^n)$, (b) holds because M_{l,n,r_n} is a function of $(A_l, S_l, M'_{l,1:n,1:r_n-1})$, (c) holds by repeating $r_n - 1$ times the steps between (6) and (7), (d) holds because $Y_n - (\bar{M}_{l,1:n-1}, X^n, Y^{n-1}) - (A_l, S_l)$, (e) holds because $(X_l)_n$ is a function of $(A_l, S_l, M'_{l,1:n-1,1:r_{n-1}})$, (f) holds by repeating $n-1$ times the steps between (6) and (8). ∎

Lemma 5. *For the non-colluding case, there exist $\hat{A}_l(V_{\mathcal{L}}, X_l^n)$, $l \in \mathcal{L}$, such that*

$$\lim_{n\to\infty} \mathbb{P}[\hat{A}_l(V_{\mathcal{L}}, X_l^n) \neq A_l] = 0, \forall l \in \mathcal{L}.$$

Proof. Let $l \in \mathcal{L}$. We suppose that Transmitter l behaves honestly during the commit phase. Define for any a_l, s_l,

$$f(a_l, s_l) \triangleq \mathbb{E}_{Y^n M_l S_l' | A_l = a_l, S_l = s_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l, s_l)\}], \qquad (9)$$

$$\mathcal{G}(a_l) \triangleq \{s_l : f(a_l, s_l) > 1 - \gamma\}, \qquad (10)$$

such that

$$
\begin{aligned}
\mathbb{P}[\mathcal{G}(a_l)] &= \mathbb{P}[f(a_l, S_l) > 1 - \gamma] \\
&= 1 - \mathbb{P}[1 - f(a_l, S_l) \geqslant \gamma] \\
&\overset{(a)}{\geqslant} 1 - \frac{\mathbb{E}_{S_l | A_l = a_l}[1 - f(a_l, S_l)]}{\gamma} \\
&\overset{(b)}{\geqslant} 1 - \delta\gamma^{-1}, \qquad (11)
\end{aligned}
$$

where (a) holds by Markov's inequality, (b) holds because by the correctness condition, for any a_l and for n large enough, we have $\mathbb{E}_{S_l | A_l = a_l} f(a_l, S_l) \geqslant 1 - \delta$.

Next, define for any x_l^n, m_l,

$$
\begin{aligned}
&F(x_l^n, m_l | a_l, s_l) \\
&\triangleq \mathbb{E}_{Y^n S_l' | M_l = m_l, X_l^n = x_l^n, S_l = s_l}[\mathbb{1}\{\beta(Y^n, m_l, S_l', a_l, s_l)\}], \qquad (12)
\end{aligned}
$$

$$F(x_l^n, m_l | a_l) \triangleq \max_{s_l \in \mathcal{G}(a_l)} F(x_l^n, m_l | a_l, s_l), \qquad (13)$$

such that for any a_l^*, s_l^*,

$$
\begin{aligned}
&\mathbb{E}_{X_l^n M_l | A_l = a_l, S_l = s_l} F(X_l^n, M_l | a_l^*, s_l^*) \\
&\overset{(a)}{=} \mathbb{E}_{X_l^n M_l | A_l = a_l, S_l = s_l} \\
&\quad \mathbb{E}_{Y^n S_l' | M_l = M_l, X_l^n = X_l^n, S_l = s_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}] \\
&= \mathbb{E}_{X_l^n | A_l = a_l, S_l = s_l} \mathbb{E}_{M_l | X_l^n = X_l^n, A_l = a_l, S_l = s_l} \\
&\quad \mathbb{E}_{Y^n S_l' | M_l = M_l, X_l^n = X_l^n, S_l = s_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}] \\
&\overset{(b)}{=} \mathbb{E}_{X_l^n | A_l = a_l, S_l = s_l} \mathbb{E}_{M_l | X_l^n = X_l^n, A_l = a_l, S_l = s_l} \\
&\quad \mathbb{E}_{Y^n S_l' | M_l = M_l, X_l^n = X_l^n, S_l = s_l, A_l = a_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}] \\
&= \mathbb{E}_{X_l^n Y^n S_l' M_l | S_l = s_l, A_l = a_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}] \\
&\overset{(c)}{=} \mathbb{E}_{Y^n S_l' M_l | S_l = s_l, A_l = a_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}], \qquad (14)
\end{aligned}
$$

where (a) holds by (12), (b) hoolds because $A_l - (M_l, X_l^n, S_l) - (Y^n, S_l')$ forms a Markov chain by Lemma 4, (c) holds by marginalization over X_l^n. Then,

$$
\begin{aligned}
&\mathbb{E}_{X_l^n M_l | A_l = a_l} F(X_l^n, M_l | a_l) \\
&\overset{(a)}{=} \mathbb{E}_{X_l^n M_l S_l | A_l = a_l} F(X_l^n, M_l | a_l) \\
&\geqslant \sum_{s_l \in \mathcal{G}(a_l)} p_{S_l | A_l = a_l}(s_l) \mathbb{E}_{X_l^n M_l | A_l = a_l, S_l = s_l} F(X_l^n, M_l | a_l) \\
&\overset{(b)}{=} \sum_{s_l \in \mathcal{G}(a_l)} p_{S_l | A_l = a_l}(s_l) \mathbb{E}_{X_l^n M_l | A_l = a_l, S_l = s_l} F(X_l^n, M_l | a_l, s_l) \\
&\overset{(c)}{=} \sum_{s_l \in \mathcal{G}(a_l)} p_{S_l | A_l = a_l}(s_l) \\
&\qquad \mathbb{E}_{Y^n S_l' M_l | S_l = s_l, A_l = a_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l, s_l)\}] \\
&\overset{(d)}{=} \sum_{s_l \in \mathcal{G}(a_l)} p_{S_l | A_l = a_l}(s_l) f(a_l, s_l) \\
&\overset{(e)}{>} \sum_{s_l \in \mathcal{G}(a_l)} p_{S_l | A_l = a_l}(s_l)(1 - \gamma) \\
&\overset{(f)}{\geqslant} (1 - \delta\gamma^{-1})(1 - \gamma), \qquad (15)
\end{aligned}
$$

where (a) holds by marginalization, (b) holds by (13), (c) holds by (14), (d) holds by (9), (e) holds by (10), (f) holds by (11). Next, define

$$\bar{F}(x_l^n, m_l | a_l) \triangleq \max_{a_l^* \neq a_l} F(x_l^n, m_l | a_l^*).$$

Then, for (a_l^*, s_l^*) such that $\bar{F}(X_l^n, M_l | a_l) = F(X_l^n, M_l | a_l^*) = F(X_l^n, M_l | a_l^*, s_l^*)$, we have

$$
\begin{aligned}
&\mathbb{E}_{X_l^n M_l | A_l = a_l}[\bar{F}(X_l^n, M_l | a_l)] \\
&\overset{(a)}{=} \mathbb{E}_{X_l^n M_l | A_l = a_l}[F(X_l^n, M_l | a_l^*, s_l^*)] \\
&\overset{(b)}{=} \mathbb{E}_{S_l | A_l = a_l} \mathbb{E}_{X_l^n M_l | A_l = a_l, S_l = S_l}[F(X_l^n, M_l | a_l^*, s_l^*)] \\
&\overset{(c)}{=} \mathbb{E}_{S_l | A_l = a_l} \mathbb{E}_{Y^n S_l' M_l | S_l = S_l, A_l = a_l}[\mathbb{1}\{\beta(Y^n, M_l, S_l', a_l^*, s_l^*)\}] \\
&\overset{(d)}{\leqslant} \delta, \qquad (16)
\end{aligned}
$$

where (a) holds by definition (a_l^*, s_l^*), (b) holds by marginalization over S_l, (c) holds by (14), (d) holds by the bindingness condition.

Finally, define

$$\hat{a}_l(x_l^n, m_l) \in \arg\max_{a_l} F(x_l^n, m_l | a_l),$$

and

$$
\begin{aligned}
&\mathbb{P}[\hat{a}_l(X_l^n, M_l) \neq a_l] \\
&= \mathbb{E}_{X_l^n M_l | A_l = a_l}[\mathbb{1}\{\hat{a}_l(X_l^n, M_l) \neq a_l\}] \\
&\leqslant \mathbb{E}_{X_l^n M_l | A_l = a_l}[\bar{F}(X_l^n, M_l | a_l) + 1 - F(X_l^n, M_l | a_l)] \\
&\xrightarrow{n\to\infty} 0,
\end{aligned}
$$

where the inequality holds because if $\hat{a}_l(x_l^n, m_l) \neq a_l$, then $F(x_l^n, m_l|a_l) \leqslant \max_{a_l^* \neq a_l} F(x_l^n, m_l|a_l^*) = \bar{F}(x_l^n, m_l|a_l)$, so that $\mathbb{1}\{\hat{a}_l(x_l^n, m_l) \neq a_l\} \leqslant \bar{F}(x_l^n, m_l|a_l) + 1 - F(x_l^n, m_l|a_l)$, and the limit holds by (15) and (16). ∎

Finally, for U uniformly distributed over $[\![1, n]\!]$ and independent of all other random variables, for any $\mathcal{T} \subseteq \mathcal{L}$, we have

$$
\begin{aligned}
& n \max_{p_{X_{\mathcal{L}}} \in \bar{\mathcal{P}}(\mathcal{X}_{\mathcal{L}})} H(X_{\mathcal{T}}|Y) \\
& \geqslant nH(X_{\mathcal{T},U}|Y_U) \\
& \overset{(a)}{\geqslant} nH(X_{\mathcal{T},U}|Y_U U) \\
& = \sum_{t=1}^{n} H(X_{\mathcal{T},t}|Y_t) \\
& \overset{(b)}{\geqslant} \sum_{t=1}^{n} H(X_{\mathcal{T},t}|Y^n X_{\mathcal{T}}^{t-1}) \\
& \overset{(c)}{=} H(X_{\mathcal{T}}^n|Y^n) \\
& \overset{(d)}{\geqslant} H(X_{\mathcal{T}}^n|V_{\mathcal{L}}) \\
& = H(X_{\mathcal{T}}^n A_{\mathcal{T}}|V_{\mathcal{L}}) - H(A_{\mathcal{T}}|X_{\mathcal{T}}^n V_{\mathcal{L}}) \\
& \overset{(e)}{\geqslant} H(X_{\mathcal{T}}^n A_{\mathcal{T}}|V_{\mathcal{L}}) - H(A_{\mathcal{T}}|\hat{A}_{\mathcal{T}}) \\
& \overset{(f)}{\geqslant} H(A_{\mathcal{T}}|V_{\mathcal{L}}) - o(n) \\
& = H(A_{\mathcal{T}}) - I(A_{\mathcal{T}}; V_{\mathcal{L}}) - o(n) \\
& \overset{(g)}{\geqslant} H(A_{\mathcal{T}}) - o(n) \\
& = nR_{\mathcal{T}} - o(n),
\end{aligned}
$$

where (a), (b), and (d) hold because conditioning reduces entropy, (c) holds by the chain rule, (e) holds with $\hat{A}_{\mathcal{T}} \triangleq (\hat{A}_l)_{l \in \mathcal{T}}$ from Lemma 5 and the data processing inequality, (f) holds by Lemma 5, (g) holds by the concealment requirement.

References

[1] M. Blum, "Coin flipping by telephone a protocol for solving impossible problems," *ACM SIGACT News*, vol. 15, no. 1, pp. 23–27, 1983.

[2] A. Winter, A. C. Nascimento, and H. Imai, "Commitment capacity of discrete memoryless channels," in *IMA International Conference on Cryptography and Coding*. Springer, 2003, pp. 35–51.

[3] C. Crépeau, "Efficient cryptographic protocols based on noisy channels," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1997, pp. 306–317.

[4] I. Damgård, J. Kilian, and L. Salvail, "On the (im) possibility of basing oblivious transfer and bit commitment on weakened security assumptions," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 56–73.

[5] I. Damgård, S. Fehr, K. Morozov, and L. Salvail, "Unfair noisy channels and oblivious transfer," in *Theory of Cryptography Conference*. Springer, 2004, pp. 355–373.

[6] H. Imai, K. Morozov, A. C. Nascimento, and A. Winter, "Efficient protocols achieving the commitment capacity of noisy correlations," in *IEEE International Symposium on Information Theory*, 2006, pp. 1432–1436.

[7] F. Oggier and K. Morozov, "A practical scheme for string commitment based on the Gaussian channel," in *IEEE Information Theory Workshop*, 2008, pp. 328–332.

[8] C. Crépeau, R. Dowsley, and A. C. Nascimento, "On the commitment capacity of unfair noisy channels," *IEEE Transactions on Information Theory*, vol. 66, no. 6, pp. 3745–3752, 2020.

[9] M. Hayashi and N. A. Warsi, "Commitment capacity of classical-quantum channels," *arXiv preprint arXiv:2201.06333*, 2022.

[10] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of computer and system sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[11] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends® in Communications and Information Theory*, vol. 4, no. 4–5, pp. 265–444, 2008.

[12] R. A. Chou, "Distributed secret sharing over a public channel from correlated random variables," *arXiv preprint arXiv:2110.10307*, 2021.

[13] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," *Combinatorial Structures and Their Applications*, 1970.