

Distributed Hypothesis Testing

With a Privacy Constraint

Sreejith Sreekumar[†], Asaf Cohen[‡] and Deniz Gündüz[†]

[†]Dept. of Electrical and Electronic Engineering, Imperial College London

[‡]Dept. of Communication Systems Engineering, Ben-Gurion University of the Negev

{s.sreekumar15,d.gunduz}@imperial.ac.uk, coasaf@bgu.ac.il

Abstract

A distributed binary hypothesis testing problem involving two parties, a remote observer and a detector, is studied. The remote observer has access to a discrete memoryless source, and communicates its observations to the detector via a rate-limited noiseless channel. The detector observes another discrete memoryless source, and performs a binary hypothesis test on the joint distribution of its own observations with those of the observer. While the goal of the observer is to maximize the type 2 error exponent of the test for a given type 1 error probability constraint, it also wants to keep a private part of its observations as oblivious to the detector as possible. Considering both equivocation and average distortion as possible measures of privacy, the trade-off between the communication rate from the observer to the detector, the type 2 error exponent and privacy is studied. For the general hypothesis testing problem, we establish single-letter inner bounds on both the rate-error exponent-equivocation and rate-error exponent-distortion trade-offs. Subsequently, single-letter characterizations for both trade-offs are obtained (i) for testing against conditional independence of the observer's observations from those of the detector, given some additional side-information at the detector; and (ii) when the communication rate constraint over the channel is zero. Finally, we show by providing a counterexample that, the strong converse which holds for distributed hypothesis testing without a privacy constraint, does not hold when a privacy constraint is imposed. This implies that, in general, the rate-error exponent-equivocation and rate-error exponent-distortion trade-offs are not independent of the type 1 error probability constraint.

I. INTRODUCTION

Data inference and privacy are often contradicting objectives. In many multi-agent system, each agent/user reveals information about its data to a remote service, application or authority, which in turn, provides certain utility to the users based on their data. Many emerging networked systems can be thought of in this context, from social networks to smart grids and communication networks. While obtaining the promised utility is the main goal of the users, privacy of data that is shared is becoming increasingly important. Thus, it is critical that users reveal only the information relevant for obtaining the desired utility, while maximum possible privacy is retained for their sensitive information.

This work has been supported in part by the European Research Council Starting Grant project BEACON (grant agreement number 677854), and by the H2020 MSCA-RISE program under project TactileNet (project ID: 690893).

In distributed learning applications, typically the goal is to learn the joint probability distribution of data available at different locations. In some cases, there may be prior knowledge about the joint distribution, for example, that it belongs to a certain set of known probability distributions. In such a scenario, the nodes communicate their observations to the detector, which then applies hypothesis testing (HT) on the underlying joint distribution of the data based on its own observations and those received from other nodes. However, with the efficient data mining and machine learning algorithms available today, the detector can illegitimately infer some unintended private information from the data provided to it exclusively for HT purposes. Such threats are becoming increasingly imminent as large amounts of seemingly irrelevant yet sensitive data are collected from users, such as in medical research [1], social networks [2], online shopping [3] and smart grids [4]. Therefore, there is an inherent trade-off between the utility acquired by sharing data and the associated privacy leakage.

In this paper, we study distributed HT with a privacy constraint, in which, an *observer* communicates its observations to a *detector* over a noiseless rate-limited channel of rate R nats per observed sample. Using the data received from the observer, the detector performs binary HT on the joint distribution of its own observations and those of the observer. The performance of the HT is measured by the asymptotic exponential rate of decay of the type 2 error probability, known as the type 2 error exponent (T2EE), for a given constraint on the type 1 error probability (definitions will be given below). While the goal is to maximize the performance of the HT, the observer also wants to maintain a certain level of privacy against the detector for some latent private data that is correlated with its observations. We are interested in characterizing the trade-off between the communication rate from the observer to the detector over the channel, T2EE achieved by the HT and the amount of information leakage of private data. A special case of HT known as *testing against conditional independence* (TACI) will be of particular interest. In TACI, the detector tests whether its own observations are independent of those at the observer, conditioned on additional side information available at the detector.

Distributed HT without any privacy constraint has been studied extensively from an information theoretic perspective in the past, although many open problems remain. The fundamental results for this problem are first established in [5], which includes a single-letter lower bound on the optimal T2EE and a *strong converse* result which states that the optimal T2EE is independent of the constraint on the type 1 error probability. Exact single-letter characterization of the optimal T2EE for the testing against independence (TAI) problem, i.e., TACI with no side information at the detector, is also obtained. The lower bound established in [5] is further improved in [6] and [7]. Strong converse is studied in the context of complete data compression and zero-rate compression in [6] and [8], respectively, where in the former, the observer communicates to the detector using a message set of size two, while in the latter using a message set whose size grows sub-exponentially with the number of observed samples. The TAI problem with multiple observers remains open (similar to several other distributed compression problems when a non-trivial fidelity criterion is involved); however, the optimal T2EE is obtained in [9] when the sources observed at different observers follow a certain Markov relation. The scenario in which, in addition to HT, the detector is also interested in obtaining a reconstruction of the observer's source, is studied in [10]. The authors characterize the trade-off between the achievable T2EE and the average distortion between the observer's observations and the detector's reconstruction. The TACI is first studied in [11], where the optimality of a random binning based encoding scheme is shown. The optimal T2EE for TACI over a noisy communication channel is established in [12]. Extension of this work to general

HT over a noisy channel is considered in [13], where lower bounds on the optimal T2EE are obtained by using a separation based scheme and also using hybrid coding for the communication between the observer and the detector. The TACI with a single observer and multiple detectors is studied in [14], where each detector tests for the conditional independence of its own observations from those of the observer. Recently, the general HT version of this problem over a noisy broadcast channel is explored in [15], where the authors employ a combination of hybrid coding and unequal error protection scheme [16]. While all the above works consider the asymmetric objective of maximizing the T2EE under a constraint on the type 1 error probability, the trade-off between the exponential rate of decay of both the type 1 and type 2 error probabilities are also considered in [17] [18] [19].

Data privacy has been a hot topic of research in the past decade, spanning across multiple disciplines in computer and computational sciences. Several practical schemes have been proposed that deals with the protection or violation of data privacy in different contexts, e.g., see [20]–[25]. More relevant for our work, HT under mutual information and maximal leakage privacy constraints have been studied in [26] and [27], respectively, where the encoder uses a *memoryless privacy mechanism* to convey a noisy version of its observed data to the detector. The detector performs HT on the probability distribution of the observer’s data, and the optimal privacy mechanism that maximizes the T2EE while satisfying the privacy constraint is analyzed. Recently, a distributed version of this problem has been studied in [28], where the goal at the detector is to perform a HT on the joint distribution of its own observations with those of the observer. In contrast with [26], [27] and [28], we study *distributed HT with a privacy constraint*, but without the restriction of memoryless coding mechanisms at the encoder. More specifically, the output of the encoder is allowed to depend on the entire sequence of observed samples, rather than a single sample. Also, while [26] and [27] are concerned with HT in a point to point setting, i.e., the detector does not have its own observations, here the focus is on distributed HT problem. In Section II, we will further discuss the differences between the system model considered here with that of [28].

Many different privacy measures have been considered in the literature to quantify the amount of private information leakage, such as k-anonymity [29], differential privacy [30], total variation distance [31] etc.; see [32] for a detailed survey. Among these, mutual information between the private and revealed information (or, equivalently, the *equivocation* of private information given the revealed information) is perhaps the most commonly used measure. It is well known that a necessary and sufficient condition to guarantee statistical independence between two random variables is to have zero mutual information between them. Furthermore, the average information leakage measured using an arbitrary privacy measure is upper bounded by a constant multiplicative factor of that measured by mutual information [33]. A rate-distortion approach to privacy is first explored by Yamamoto in [34] for a rate-constrained noiseless channel where, in addition to a distortion constraint for legitimate data, a minimum distortion requirement is enforced for the private part. Other measures of information leakage that are stronger than mutual information has been recently considered in [35]. In this paper, we will consider both equivocation and average distortion as the measures of privacy. In [36], the T2EE of a HT adversary is considered as a privacy measure. This can be considered as the opposite setting to ours, in the sense that, while the goal here is to increase the T2EE under a privacy leakage constraint, the goal in [36] is to reduce the T2EE under a constraint on possible transformations that can be applied on the data.

The amount of private information leakage that can be tolerated depends on the specific application at hand. While it may be possible to tolerate a moderate amount of private information leakage in applications like online shopping or social networks, it may no longer be the case in matters related to information sharing among government agencies or corporates. While it is obvious that maximum privacy can be attained by revealing no information, this typically comes at the cost of zero utility. On the other hand, maximum utility can be achieved by revealing all the information, but at the cost of minimum privacy. Characterizing the optimal trade-off between the utility and the minimum privacy leakage between these two extremes is a challenging research problem.

It is important to note here that the data privacy problem is fundamentally different from that of data security against an eavesdropper or an adversary. In data security, sensitive data is to be protected against an external malicious agent distinct from the legitimate parties in the system. The techniques for guaranteeing data security usually involve either cryptographic methods in which the legitimate parties are assumed to have additional resources unavailable to the adversary (e.g., a shared private key) or the availability of better communication channel conditions. However, in data privacy problems, the sensitive data is to be protected from the same legitimate party that provides the utility; and hence, the above mentioned techniques for guaranteeing data security are not applicable.

Main Contributions

The main contributions of this work are as follows.

- (i) In Section III, Theorem 8 (resp. Theorem 9), we establish a single-letter inner bound on the rate-T2EE-equivocation (resp. rate-T2EE-distortion) trade-off for distributed HT with a privacy constraint.
- (ii) Exact characterizations are obtained for some important special cases in Section IV. More specifically, a single-letter characterization of the optimal rate-T2EE-equivocation (resp. rate-T2EE-distortion) trade-off is established for:
 - a) TACI with a privacy constraint (for vanishing type 1 error probability constraint) in Section IV-A, Theorem 10 (resp. Theorem 11).
 - b) distributed HT with a privacy constraint for zero-rate compression ($R = 0$) in Section IV-B, Theorem 15 (resp. Theorem 14).

Since the optimal trade-offs in Theorem 14 and Theorem 15 are independent of the constraint on the type 1 error probability, they are strong converse results in the context of HT.

- (iii) Finally, in Section V, we provide a counterexample showing that for positive rate $R > 0$, the strong converse result does not hold in general for TAI with a privacy constraint.

The organization of the paper is as follows. The basic notations are introduced in Section II-A. The problem formulation and associated definitions are given in Section II-B. The results are presented in Sections III to V. The proofs of the results are presented either in the Appendix or immediately after the statement of the result. Finally, Section VI concludes the paper with some open problems for future research.

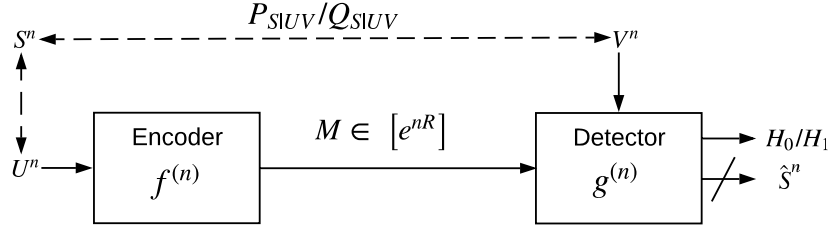


Fig. 1: HT with a privacy constraint.

II. PRELIMINARIES

A. Notations

All the random variables (r.v.'s) considered in this paper are discrete with finite support unless specified otherwise. We denote r.v.'s and their realizations by upper and lower case letters (e.g., X and x), respectively. Sets are denoted by calligraphic letters, e.g., the alphabet of a r.v. X is denoted by \mathcal{X} . Sequence of r.v.'s (X_1, \dots, X_n) will be denoted by X^n . The group of m r.v.'s $X_{(j-1)m+1}, \dots, X_{jm}$ is denoted by $X^m(j)$, and the infinite sequence $X^m(1), X^m(2), \dots$ is denoted by $\{X^m(j)\}_{j \in \mathbb{Z}^+}$. $D(P_X || Q_X)$, $H_{P_X}(X)$, $H_{P_{XY}}(X|Y)$ and $I_{P_{XY}}(X; Y)$ represent the standard quantities of Kullback-Leibler (KL) divergence between distributions P_X and Q_X , the entropy of X with distribution P_X , the conditional entropy of X given Y and the mutual information between X and Y with joint distribution P_{XY} , respectively. When the distribution of the r.v.'s involved are clear from the context, the entropic and mutual information quantities are denoted simply by $I(X; Y)$, $H(X)$ and $H(X|Y)$, respectively. Following the notation in [37], T_P and $T_{[P_X]_\delta}^m$ (or $T_{[X]_\delta}^m$ or T_δ^m when there is no ambiguity) denote the set of sequences of type P and the set of P_X -typical sequences of length m , respectively. The set of all types of k -length sequences of r.v.'s X^k and Y^k is denoted by $\mathcal{T}^k(\mathcal{X} \times \mathcal{Y})$ and $\cup_{k \in \mathbb{Z}^+} \mathcal{T}^k(\mathcal{X} \times \mathcal{Y})$ is denoted by $\mathcal{T}(\mathcal{X} \times \mathcal{Y})$. Given realizations $X^n = x^n$ and $Y^n = y^n$, $H_e(x^n|y^n)$ denotes the conditional empirical entropy defined as

$$H_e(x^n|y^n) := H_{P_{\tilde{X}\tilde{Y}}}(X|Y)$$

where $P_{\tilde{X}\tilde{Y}}$ denotes the joint type of (x^n, y^n) . $\mathbb{1}$ denotes the indicator function. $X - Y - Z$ denotes a Markov chain between the r.v.'s X , Y and Z , while $X \perp Y$ denotes statistical independence between X and Y . $\xrightarrow{(n)}$ denotes asymptotic limit with respect to n , e.g., $a_n \xrightarrow{(n)} 0$ means the sequence a_n tends to zero asymptotically with n . $\mathbb{P}(\mathcal{E})$ denotes the probability of event \mathcal{E} . For positive real m , we define $[m] := \{1, \dots, [m]\}$. For an arbitrary set \mathcal{A} , we denote its complement by \mathcal{A}^c , and for $\mathcal{A} \subseteq \mathbb{R}^n$, we denote its interior and closure by $int(\mathcal{A})$ and $cl(\mathcal{A})$ (with respect to the Euclidean metric), respectively. Whenever the range of the summation is not specified, this will mean summation over the entire support, e.g., \sum_u denotes $\sum_{u \in \mathcal{U}}$, unless specified otherwise. Throughout this paper, the base of the logarithms is taken to be e . For $a \in \mathbb{R}$, a^+ denotes $\max\{0, a\}$. For two probability distributions P and Q defined on a common support \mathcal{X} , $P \ll Q$ will mean that P is absolutely continuous with respect to Q .

B. Problem formulation

Consider the HT setup illustrated in Fig. 1. The encoder (observer) observes a discrete memoryless source U^n and sends the message index $M := f^{(n)}(U^n)$ to the detector over an error-free channel using some encoding function (possibly stochastic) $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$. Given its own independent and identically distributed (i.i.d.) observation V^n , the detector performs a HT on the joint distribution¹ of U^n and V^n with null hypothesis

$$H_0 : (U^n, V^n) \sim \prod_{i=1}^n P_{UV},$$

and alternate hypothesis

$$H_1 : (U^n, V^n) \sim \prod_{i=1}^n Q_{UV}.$$

Let $H, \hat{H} \in \{0, 1\}$ denote the r.v.'s corresponding to the true hypothesis and the output of the HT, respectively, where 0 denotes the null hypothesis and 1 the alternate hypothesis. Let $g^{(n)} : \mathcal{M} \times \mathcal{V}^n \rightarrow \{P_{\hat{H}|M, V^n}\}$ denote the decision rule at the detector. The type 1 and type 2 error probability for an $(f^{(n)}, g^{(n)})$ pair are defined as

$$\bar{\alpha}(f^{(n)}, g^{(n)}) := \mathbb{P}(\hat{H} = 1 | H = 0) = P_{\hat{H}}(1),$$

and

$$\bar{\beta}(f^{(n)}, g^{(n)}) := \mathbb{P}(\hat{H} = 0 | H = 1) = Q_{\hat{H}}(0),$$

respectively, where

$$P_{\hat{H}}(1) = \sum_{u^n, m, v^n} \left[\prod_{i=1}^n P_{UV}(u_i, v_i) \right] P_{M|U^n}(m|u^n) P_{\hat{H}|MV^n}(1|m, v^n),$$

$$\text{and } Q_{\hat{H}}(0) = \sum_{u^n, m, v^n} \left[\prod_{i=1}^n Q_{UV}(u_i, v_i) \right] P_{M|U^n}(m|u^n) P_{\hat{H}|MV^n}(0|m, v^n).$$

For a given type 1 error probability constraint ϵ , define the minimum type 2 error probability over all possible detectors as

$$\beta(f^{(n)}, \epsilon) := \inf_{g^{(n)}} \bar{\beta}(f^{(n)}, g^{(n)}), \quad (1)$$

such that $\bar{\alpha}(f^{(n)}, g^{(n)}) \leq \epsilon$.

The performance of HT is measured by the T2EE achieved by the test for a given constraint ϵ on the type 1 error probability, i.e., $\liminf_{n \rightarrow \infty} -\frac{1}{n} \log(\beta(f^{(n)}, \epsilon))$. Although the goal of the detector is to maximize the T2EE achieved for the HT, it is also curious about a latent r.v. S^n that is correlated with the source U^n . S^n is referred to as the *private* part of U^n , which is distributed i.i.d. according to the joint distribution P_{SUV} and Q_{SUV} under the null and alternate hypothesis, respectively. It is desired to keep the private part as concealed as possible from the detector. We consider two measures of privacy for S^n at the

¹Although a r.v. is specified together with its probability distribution, here, we abuse the notation for ease of exposition, and denote the observations at the observer and detector under both the null and alternate hypothesis by (U^n, V^n) , with probability distribution $\prod_{i=1}^n P_{UV}$ and $\prod_{i=1}^n Q_{UV}$, respectively. This terminology is used throughout the paper.

detector. The first is the *equivocation* defined as $\frac{1}{n}H(S^n|M, V^n)$. The second one is the *average distortion* between S^n and its reconstruction \hat{S}^n at the detector, measured according to an arbitrary bounded additive distortion metric $d : \mathcal{S} \times \hat{\mathcal{S}} \rightarrow [0, D_m]$ with multi-letter distortion defined as

$$d(s^n, \hat{s}^n) := \frac{1}{n} \sum_{i=1}^n d(s_i, \hat{s}_i).$$

The goal is to ensure that the T2EE for HT is maximized, while satisfying the constraints on the type 1 error probability ϵ and the privacy of S^n . In the sequel, we study the trade-off between the rate, T2EE (henceforth also referred to simply as the error exponent) and privacy achieved in the above setting. Before delving into that, a few definitions are in order.

Definition 1. For a given type 1 error probability constraint ϵ , a rate-error exponent-distortion tuple $(R, \kappa, \Delta_0, \Delta_1)$ is achievable, if there exists a sequence of encoding and decoding functions $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$ and $g^{(n)} : [e^{nR}] \times \mathcal{V}^n \rightarrow \{P_{\hat{H}|M, V^n}\}$ such that

$$\limsup_{n \rightarrow \infty} \frac{\log(\beta(f^{(n)}, \epsilon))}{n} \leq -\kappa, \text{ and} \quad (2)$$

$$\liminf_{n \rightarrow \infty} \inf_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = i \right] \geq \Delta_i, \quad i = 0, 1, \quad (3)$$

where $g_r^{(n)} : [e^{nR}] \times \mathcal{V}^n \rightarrow \{P_{\hat{S}^n|M, V^n}\}$ and $P_{\hat{S}^n|M, V^n}$ denotes an arbitrary conditional probability distribution. The rate-error exponent-distortion region $\mathcal{R}_d(\epsilon)$ is the closure of the set of all such achievable $(R, \kappa, \Delta_0, \Delta_1)$ tuples for a given ϵ .

Definition 2. For a given type 1 error probability constraint ϵ , a rate-error exponent-equivocation $(R, \kappa, \Omega_0, \Omega_1)$ tuple is achievable, if there exists a sequence of encoding and decoding functions $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$ and $g^{(n)} : [e^{nR}] \times \mathcal{V}^n \rightarrow \{P_{\hat{H}|M, V^n}\}$ such that (2) is satisfied and

$$\liminf_{n \rightarrow \infty} \frac{1}{n} H(S^n|M, V^n, H = i) \geq \Omega_i, \quad i = 0, 1. \quad (4)$$

The rate-error exponent-equivocation region $\mathcal{R}_e(\epsilon)$ is the closure of the set of all achievable $(R, \kappa, \Omega_0, \Omega_1)$ tuples for a given ϵ .

Before stating our results, we briefly highlight the differences between our system model and the one studied in [28]. In [28], the observer applies a memoryless privacy mechanism to the data before releasing it to the transmitter, which performs further encoding prior to transmission to the detector, while in our model, there is no such restriction, as is obvious from the definitions above. Also, while we consider the equivocation (or average distortion) between the revealed information and the private part as the privacy measure, in [28], the mutual information between the observer's observations and the output of the memoryless mechanism is the privacy measure. Thus, perfect privacy in their model would imply that the T2EE is also zero, since the output of the memoryless mechanism has to be independent of the observer's observations (under both hypothesis). However, as we show in Example 1 later, a positive T2EE is achievable while guaranteeing perfect privacy in our model.

Next, we state some supporting results that will be useful later for proving the main results.

C. Supporting Results

First, we show that restricting our attention to a deterministic detector $g^{(n)} : [e^{nR}] \times \mathcal{V}^n \rightarrow \{0, 1\}$ in Definitions 1 and 2 is without loss of optimality. Accordingly, let

$$g^{(n)}(m, v^n) = \mathbb{1} \left((m, v^n) \in \mathcal{A}_{(n)}^c \right) \quad (5)$$

denote the deterministic detector with acceptance region $\mathcal{A}_{(n)} \subseteq [e^{nR}] \times \mathcal{V}^n$ for H_0 and $\mathcal{A}_{(n)}^c$ for H_1 . Then, the type 1 and type 2 error probabilities are given by

$$\bar{\alpha} \left(f^{(n)}, g^{(n)} \right) := P_{MV^n}(\mathcal{A}_{(n)}^c) = \mathbb{E} \left(\mathbb{1}(M, V^n) \in \mathcal{A}_{(n)}^c | H = 0 \right), \quad (6)$$

$$\bar{\beta} \left(f^{(n)}, g^{(n)} \right) := Q_{MV^n}(\mathcal{A}_{(n)}) = \mathbb{E} \left(\mathbb{1}(M, V^n) \in \mathcal{A}_{(n)} | H = 1 \right). \quad (7)$$

Proposition 3. *It is sufficient to consider a deterministic detector of the form given in (5) for some $\mathcal{A}_{(n)} \subseteq [e^{nR}] \times \mathcal{V}^n$, where $\mathcal{A}_{(n)}$ and $\mathcal{A}_{(n)}^c$ denote the acceptance regions for H_0 and H_1 , respectively.*

Proof: Note that for a stochastic detector, the type 1 and type 2 error probabilities are linear functions of $P_{\hat{H}|MV^n}$. As a result, for each fixed n and $f^{(n)}$, $\bar{\alpha} \left(f^{(n)}, g^{(n)} \right)$ and $\bar{\beta} \left(f^{(n)}, g^{(n)} \right)$ for a stochastic detector $g^{(n)}$ can be thought of as the type 1 and type 2 errors achieved by "time sharing" among a finite number of deterministic detectors. Now, suppose $(\bar{\alpha}_1^{(n)}, \bar{\beta}_1^{(n)})$ and $(\bar{\alpha}_2^{(n)}, \bar{\beta}_2^{(n)})$ denote the pair of type 1 and type 2 error probabilities achieved by deterministic detectors $g_1^{(n)}$ and $g_2^{(n)}$, respectively. Let $\mathcal{A}_{1,(n)}$ and $\mathcal{A}_{2,(n)}$ denote their corresponding acceptance regions for H_0 . Let $g_\theta^{(n)}$ denote the stochastic detector formed by using $g_1^{(n)}$ and $g_2^{(n)}$ with probabilities θ and $1 - \theta$, respectively. From the above mentioned linearity property, it follows that $g_\theta^{(n)}$ achieves type 1 and type 2 error probabilities of $\bar{\alpha} \left(f^{(n)}, g_\theta^{(n)} \right) = \theta \bar{\alpha}_1^{(n)} + (1 - \theta) \bar{\alpha}_2^{(n)}$ and $\bar{\beta} \left(f^{(n)}, g_\theta^{(n)} \right) = \theta \bar{\beta}_1^{(n)} + (1 - \theta) \bar{\beta}_2^{(n)}$, respectively. Note that for $\theta \in (0, 1)$, the exponent of the type 2 error probability for $(f^{(n)}, g_\theta^{(n)})$ pair is given by

$$-\frac{1}{n} \log \left(\bar{\beta} \left(f^{(n)}, g_\theta^{(n)} \right) \right) = \min \left(-\frac{1}{n} \log \left(\bar{\beta}_1^{(n)} \left(f^{(n)}, g_1^{(n)} \right) \right), -\frac{1}{n} \log \left(\bar{\beta}_2^{(n)} \left(f^{(n)}, g_2^{(n)} \right) \right) \right).$$

Hence, either

$$\bar{\alpha}_1^{(n)} \leq \bar{\alpha} \left(f^{(n)}, g_\theta^{(n)} \right) \quad \text{and} \quad -\frac{1}{n} \log \left(\bar{\beta}_1^{(n)} \left(f^{(n)}, g_1^{(n)} \right) \right) \geq -\frac{1}{n} \log \left(\bar{\beta} \left(f^{(n)}, g_\theta^{(n)} \right) \right),$$

or

$$\bar{\alpha}_2^{(n)} \leq \bar{\alpha} \left(f^{(n)}, g_\theta^{(n)} \right) \quad \text{and} \quad -\frac{1}{n} \log \left(\bar{\beta}_2^{(n)} \left(f^{(n)}, g_2^{(n)} \right) \right) \geq -\frac{1}{n} \log \left(\bar{\beta} \left(f^{(n)}, g_\theta^{(n)} \right) \right).$$

Thus, a stochastic detector does not offer any advantage over deterministic detectors in the trade-off between the T2EE and the type 1 error probability. ■

Due to Proposition 3, henceforth we restrict our attention to deterministic $g^{(n)}$. The next result shows that without loss of

generality (w.l.o.g), it is also sufficient to consider $g_r^{(n)}$ (in Definition 1) to be a deterministic function of the form

$$g_r^{(n)} = \{\phi_i(m, v^n)\}_{i=1}^n, \quad (8)$$

for the minimization in (3), where $\phi_i : \mathcal{M} \times \mathcal{V}^n \rightarrow \hat{\mathcal{S}}$, $i \in [1 : n]$, denotes an arbitrary deterministic function.

Proposition 4. *For the minimization in (3), it is sufficient to restrict our attention to a deterministic function $g_r^{(n)}$ as given in (8).*

Proof: Let $\tilde{P}_{S^n U^n V^n M}^{(j)}$ denote the joint distribution of the r.v.'s (S^n, U^n, V^n, M) under hypothesis H_j , $j = 0, 1$, and $\tilde{P}_{\hat{S}^n | M, V^n}$ denote an arbitrary stochastic function for $g_r^{(n)}$. Then, we have

$$\begin{aligned} \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = j \right] &= \min_{\tilde{P}_{\hat{S}^n | M, V^n}} \mathbb{E}_{\tilde{P}^{(j)}} \left[d(S^n, \hat{S}^n) \right] \\ &= \min_{\{\tilde{P}_{\hat{S}_i | M, V^n}\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(j)}} \left[d(S_i, \hat{S}_i) \right] \\ &= \frac{1}{n} \sum_{i=1}^n \sum_{M=m, V^n=v^n} \tilde{P}_{MV^n}^{(j)}(m, v^n) \min_{\hat{S}_i} \sum_{\hat{S}_i} \tilde{P}_{\hat{S}_i | M=m, V^n=v^n}(\hat{S}_i) \mathbb{E}_{\tilde{P}_{\hat{S}_i | M=m, V^n=v^n}^{(j)}} [d(S_i, \hat{S}_i)] \\ &= \frac{1}{n} \sum_{i=1}^n \sum_{M=m, V^n=v^n} \tilde{P}_{MV^n}^{(j)}(m, v^n) \mathbb{E}_{\tilde{P}_{\hat{S}_i | M=m, V^n=v^n}^{(j)}} [d(S_i, \phi_{ij}(m, v^n))], \end{aligned}$$

where,

$$\phi_{ij}(m, v^n) = \arg \min_{\hat{S}_i \in \hat{\mathcal{S}}} \mathbb{E}_{\tilde{P}_{\hat{S}_i | M=m, V^n=v^n}^{(j)}} [d(S_i, \hat{S}_i)].$$

Continuing, we have

$$\begin{aligned} \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = j \right] &= \frac{1}{n} \sum_{i=1}^n \sum_{M=m, V^n=v^n} \tilde{P}_{MV^n}^{(j)}(m, v^n) \min_{\phi_i(m, v^n)} \mathbb{E}_{\tilde{P}_{\hat{S}_i | M=m, V^n=v^n}^{(j)}} [d(S_i, \phi_i(m, v^n))] \\ &= \min_{\{\phi_i(m, v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(j)}} [d(S_i, \phi_i(M, V^n))]. \end{aligned} \quad (9)$$

■

Next, we state some lemmas that will be handy for upper bounding the amount of privacy leakage in the proofs of the main results stated below. The following one is a well known result proved in [37] that upper bounds the difference in entropy of two r.v.'s (with a common support) in terms of the total variation distance between their probability distributions.

Definition 5. *The total variation between probability distributions P_X and Q_X defined on the same support \mathcal{X} is defined as*

$$\|P_X - Q_X\| = \frac{1}{2} \sum_{x \in \mathcal{X}} |P_X(x) - Q_X(x)|.$$

Lemma 6. [37, Lemma 2.7] *Let P_X and Q_X be distributions defined on a common support \mathcal{X} and let $\rho := \|P_X - Q_X\|$.*

Then,

$$|H_{P_X} - H_{Q_X}| \leq -2\rho \log \left(\frac{2\rho}{|\mathcal{X}|} \right).$$

The next lemma will be used later in the proofs of Theorem 8, Theorem 9, Theorem 14 and counter-example for strong converse in Section V.

Lemma 7. Let P_{XY} and Q_{XY} denote two arbitrary joint probability distributions of the r.v.'s X and Y . Let $P_{X^n Y^n} = \prod_{i=1}^n P_{XY}$ and $Q_{X^n Y^n} = \prod_{i=1}^n Q_{XY}$ denote probability distributions of the r.v.'s X^n and Y^n . For $\delta > 0$, define

$$I_X(x^n, \delta) := \mathbb{1} \left(x^n \notin T_{[P_X]_\delta}^n \right). \quad (10)$$

If $P_X \neq Q_X$, then for $\delta > 0$ sufficiently small,

$$\|Q_{Y^n} - Q_{Y^n|I_X(X^n, \delta)=1}\| \xrightarrow{(n)} 0. \quad (11)$$

If $P_X = Q_X$, then the following holds for any $\delta > 0$,

$$\|Q_{Y^n} - Q_{Y^n|I_X(X^n, \delta)=0}\| \xrightarrow{(n)} 0, \quad (12)$$

$$\|P_{Y^n} - P_{Y^n|I_X(X^n, \delta)=0}\| \xrightarrow{(n)} 0. \quad (13)$$

Proof: The proof is presented in Appendix A. ■

To provide further intuition into the claims given in (11)-(13) of Lemma 7, we briefly explain each of them. Eqn. (11) states that if the marginals P_X and Q_X are different, then the conditional distribution Q_{Y^n} of Y^n given that $X^n \notin T_{[P_X]_\delta}^n$, is close (in terms of total variation distance) to the unconditional distribution Q_{Y^n} , provided that δ is small enough. This essentially means that the conditional distribution Q_{Y^n} , conditioned on the knowledge that X^n is not P_X -typical, does not differ much from the unconditional distribution asymptotically. Similarly, (12) and (13), respectively, state that given $P_X = Q_X$, the conditional distribution Q_{Y^n} (resp. P_{Y^n}) of Y^n given that $X^n \in T_{[P_X]_\delta}^n$, is close to the unconditional distribution Q_{Y^n} (resp. P_{Y^n}) for any value of $\delta > 0$. This implies that the knowledge of X^n being P_X -typical does not change the marginal distribution of Y^n by much asymptotically.

In the next section, we establish an inner bound on $\mathcal{R}_e(\epsilon)$ and $\mathcal{R}_d(\epsilon)$.

III. MAIN RESULTS

The following two theorems are the main results of this paper providing inner bounds for $\mathcal{R}_e(\epsilon)$ and $\mathcal{R}_d(\epsilon)$, respectively.

Theorem 8. For $\epsilon \in (0, 1)$, $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$ if there exists an auxiliary r.v. W , such that $(V, S) - U - W$, and

$$R \geq I_P(W; U|V), \quad (14)$$

$$\kappa \leq \kappa^*(P_{W|U}, R), \quad (15)$$

$$\Omega_0 \leq H_P(S|W, V), \quad (16)$$

$$\Omega_1 \leq \mathbb{1}(P_U = Q_U) H_Q(S|W, V) + \mathbb{1}(P_U \neq Q_U) H_Q(S|V), \quad (17)$$

where

$$\begin{aligned} \kappa^*(P_{W|U}, R) &:= \min (E_1(P_{W|U}), E_2(R, P_{W|U})), \\ E_1(P_{W|U}) &:= \min_{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{T}_1(P_{UW}, P_{VW})} D(P_{\tilde{U}\tilde{V}\tilde{W}} || Q_{UV} P_{W|U}), \end{aligned} \quad (18)$$

$$E_2(R, P_{W|U}) := \begin{cases} \min_{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{T}_2(P_{UW}, P_V)} D(P_{\tilde{U}\tilde{V}\tilde{W}} || Q_{UV} P_{W|U}) + (R - I_P(U; W|V)), & \text{if } I_P(U; W) > R, \\ \infty, & \text{otherwise,} \end{cases} \quad (19)$$

$$\mathcal{T}_1(P_{UW}, P_{VW}) := \{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{T}(\mathcal{U} \times \mathcal{V} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW}, P_{\tilde{V}\tilde{W}} = P_{VW}\},$$

$$\mathcal{T}_2(P_{UW}, P_V) := \{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{T}(\mathcal{U} \times \mathcal{V} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW}, P_{\tilde{V}} = P_V, H_P(W|V) \leq H(\tilde{W}|\tilde{V})\},$$

$$P_{SUVW} := P_{SUV} P_{W|U}, \quad Q_{SUVW} := Q_{SUV} P_{W|U}.$$

Theorem 8 is the direct part or the achievability result in the parlance of information theory, and utilizes the well-known coding techniques of quantization and binning, along with minimum empirical entropy decoding using the available side-information at the detector. While the analysis of the T2EE is similar to that of the Shimokawa-Han-Amari scheme [7], the analysis of the privacy part is new. Indeed, we recover the rate-T2EE trade-off derived in [7] when the privacy constraint in Theorem 8 is relaxed. The detailed proof of Theorem 8 is presented in Appendix B. We next state an inner bound for $\mathcal{R}_d(\epsilon)$.

Theorem 9. For a given bounded additive distortion measure $d(\cdot, \cdot)$ and $\epsilon \in (0, 1)$, $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$ if there exist an auxiliary r.v. W and deterministic functions $\phi : \mathcal{W} \times \mathcal{V} \rightarrow \hat{S}$ and $\phi' : \mathcal{V} \rightarrow \hat{S}$, such that $(V, S) - U - W$ and (14), (15),

$$\Delta_0 \leq \min_{\phi(\cdot, \cdot)} \mathbb{E}_P [d(S, \phi(W, V))], \quad (20)$$

$$\text{and } \Delta_1 \leq \mathbb{1}(P_U = Q_U) \min_{\phi(\cdot, \cdot)} \mathbb{E}_Q [d(S, \phi(W, V))] + \mathbb{1}(P_U \neq Q_U) \min_{\phi'(\cdot)} \mathbb{E}_Q [d(S, \phi'(V))], \quad (21)$$

are satisfied, where P_{SUVW} and Q_{SUVW} are as defined in Theorem 8.

The proof of Theorem 9 is presented in Appendix C. We mention an important point regarding average distortion as a privacy measure. In order to obtain a single-letter lower bound for the achievable distortion of the private part at the detector, it is required that the a posteriori probability distribution of S^n given the observations (M, V^n) at the detector is close in some sense to a desired ‘‘target’’ memoryless distribution (as will become apparent from the proof). For this purpose, we use stochastic encoding to induce the necessary randomness for S^n at the detector. The analysis of the joint distribution of the r.v.’s in the system (both the given r.v.’s and those generated as part of the coding scheme) is done using the so-called channel resolvability or soft-covering lemma [38]–[40]. Properties of the total variation distance between probability distributions play a key role in this analysis.

Theorems 8 and 9 provide single-letter inner bounds on $\mathcal{R}_d(\epsilon)$ and $\mathcal{R}_e(\epsilon)$, respectively. A complete computable characterization of these regions would require a matching converse. This is a hard problem, since such a characterization is not available even for the distributed HT problem in general, without a privacy constraint (see [5]). However, it is known that a

single-letter characterization of the rate-error exponent region exists for the special case of TACI [11]. In the next section, we show that TACI with a privacy constraint also admits a single-letter characterization, in addition to other optimality results.

IV. OPTIMALITY RESULTS FOR SPECIAL CASES

A. TACI with a Privacy Constraint

Assume that the detector observes two discrete memoryless sources Y^n and Z^n , i.e., $V^n = (Y^n, Z^n)$. In TACI, the detector tests for the conditional independence of U and Y , given Z . Thus, the joint distribution of the r.v.'s under the null and alternate hypothesis are given by

$$H_0 : P_{SUYZ} := P_{S|UYZ}P_{U|Z}P_{Y|UZ}P_Z, \quad (22)$$

and

$$H_1 : Q_{SUYZ} := Q_{S|UYZ}P_{U|Z}P_{Y|Z}P_Z, \quad (23)$$

respectively.

Let \mathcal{R}_e and \mathcal{R}_d denote the rate-error exponent-equivocation and rate-error exponent-distortion regions, respectively, for the case of vanishing type 1 error probability constraint, i.e.,

$$\mathcal{R}_e := \lim_{\epsilon \rightarrow 0} \mathcal{R}_e(\epsilon) \text{ and } \mathcal{R}_d := \lim_{\epsilon \rightarrow 0} \mathcal{R}_d(\epsilon).$$

Assume that the privacy constraint under the alternate hypothesis is inactive. Thus, we are interested in characterizing the set of all tuples $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e$ and $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d$, where

$$\begin{aligned} \Omega_1 &\leq \Omega_{min} := H_Q(S|U, Y, Z), \\ \text{and } \Delta_1 &\leq \Delta_{min} := \min_{\phi(u,y,z)} \mathbb{E}_Q [d(S, \phi(U, Y, Z))]. \end{aligned} \quad (24)$$

Note that Ω_{min} and Δ_{min} correspond to the equivocation and average distortion of S^n at the detector, respectively, when U^n is available directly at the detector under the alternate hypothesis. The above assumption is motivated by scenarios, in which, the encoder is more eager to protect S^n when there is a correlation between its own observation and that of the decoder. Consider the following example of user privacy in the context of online shopping, in which the encoder and detector correspond to a consumer and an online shopping portal, respectively. A consumer would like to share some information about his/her shopping behaviour, e.g., shopping history and preferences, with the shopping portal in order to get better deals and recommendations on relevant products. The shopping portal would like to determine whether the consumer belongs to its target age group (e.g., below 30 years old) before sending special offers to this customer. Assuming that the shopping patterns of the users within and outside the target age groups are independent, the shopping portal performs an independence test to check if the consumer's shared data is correlated with the data of its own customers. If the consumer is indeed within the target age group, the shopping portal would like to gather more information about this potential customer, particular interests, more accurate age estimation,

etc.; while the user is reluctant to provide any further information. In this example, U^n , S^n and Y^n corresponds to shopping behaviour, more information about the customer, and customers data available to the shopping portal, respectively.

For the above mentioned case, we have the following results.

Theorem 10. $(R, \kappa, \Omega_0, \Omega_{min}) \in \mathcal{R}_e$ if and only if there exists an auxiliary r.v. W , such that $(Z, Y, S) - U - W$, and

$$\kappa \leq I_P(W; Y|Z), \quad (25)$$

$$R \geq I_P(W; U|Z), \quad (26)$$

$$\Omega_0 \leq H_P(S|W, Z, Y), \quad (27)$$

for some joint distribution of the form $P_{SUYZW} := P_{SUYZ}P_{W|U}$.

Proof: For TACI, the inner bound in Theorem 8 yields that for $\epsilon \in (0, 1)$, $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$ if there exists an auxiliary r.v. W , such that $(Y, Z, S) - U - W$, and

$$R \geq I_P(W; U|Y, Z), \quad (28)$$

$$\kappa \leq \kappa^*(P_{W|U}, R), \quad (29)$$

$$\Omega_0 \leq H_P(S|W, Y, Z), \quad (30)$$

$$\Omega_1 \leq H_Q(S|W, Y, Z), \quad (31)$$

where

$$\kappa^*(P_{W|U}, R) := \min(E_1(P_{W|U}), E_2(R, P_{W|U})),$$

$$E_1(P_{W|U}) := \min_{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{T}_1(P_{UW}, P_{YZ})} D(P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \| Q_{UYZ} P_{W|U}), \quad (32)$$

$$E_2(R, P_{W|U}) := \begin{cases} \min_{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{T}_2(P_{UW}, P_{YZ})} D(P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \| Q_{UYZ} P_{W|U}) + (R - I_P(U; W|Y, Z)), & \text{if } I_P(U; W) > R, \\ \infty, & \text{otherwise,} \end{cases} \quad (33)$$

$$\mathcal{T}_1(P_{UW}, P_{YZ}) := \{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{T}(\mathcal{U} \times \mathcal{Y} \times \mathcal{Z} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW}, P_{\tilde{Y}\tilde{Z}\tilde{W}} = P_{YZ}\},$$

$$\mathcal{T}_2(P_{UW}, P_{YZ}) := \{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{T}(\mathcal{U} \times \mathcal{Y} \times \mathcal{Z} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW}, P_{\tilde{Y}\tilde{Z}} = P_{YZ}, H_P(W|Y, Z) \leq H(\tilde{W}|\tilde{Y}\tilde{Z})\},$$

$$P_{SUYZW} := P_{SUYZ}P_{W|U}, Q_{SUYZW} := Q_{S|YZ}P_{U|Z}P_{Y|Z}P_Z P_{W|U}.$$

Note that since $(Y, Z, S) - U - W$, we have

$$I_P(W; U) \geq I_P(W; U|Z) \geq I_P(W; U|Y, Z). \quad (34)$$

Let $\mathcal{B}' := \{P_{W|U} : I_P(U; W|Z) \leq R\}$. Then, for $P_{W|U} \in \mathcal{B}'$, we have,

$$\begin{aligned} E_1(R, P_{W|U}) &= \min_{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{T}_1(P_{UW}, P_{YZW})} D(P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \| Q_{UYZ} P_{W|U}) = I_P(Y; W|Z), \\ E_2(R, P_{W|U}) &\geq I_P(U; W|Z) - I_P(U; W|Y, Z) = I_P(Y; W|Z). \end{aligned}$$

Hence,

$$\kappa^*(P_{W|U}, R) \geq I_P(Y; W|Z). \quad (35)$$

By noting that $\Omega_{min} \leq H_Q(S|W, Y, Z)$ (by the data processing inequality), we have shown that for $\Omega_1 \leq \Omega_{min}$, $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e$ if (25)-(27) are satisfied. This completes the proof of achievability.

Converse: Let $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e$. Let T be a r.v. uniformly distributed over $[n]$ and independent of all the other r.v.'s (U^n, Y^n, Z^n, M) . Define an auxiliary r.v. $W := (W_T, T)$, where $W_i := (M, Y^{i-1}, Z^{i-1}, Z_{i+1}^n)$, $i \in [n]$. Note that $(Z, Y) - U - W$. Then, for any $\gamma' > 0$ and sufficiently large n , we have

$$\begin{aligned} n(R + \gamma') &\geq H_P(M) \geq H_P(M|Z^n) \geq I_P(M; U^n|Z^n) \\ &= \sum_{i=1}^n I_P(M; U_i|U^{i-1}, Z^n) \\ &= \sum_{i=1}^n I_P(M, U^{i-1}, Z^{i-1}, Z_{i+1}^n; U_i|Z_i) \end{aligned} \quad (36)$$

$$= \sum_{i=1}^n I_P(M, U^{i-1}, Z^{i-1}, Z_{i+1}^n, Y^{i-1}; U_i|Z_i) \quad (37)$$

$$\geq \sum_{i=1}^n I_P(M, Z^{i-1}, Z_{i+1}^n, Y^{i-1}; U_i|Z_i)$$

$$= \sum_{i=1}^n I_P(W_i; U_i|Z_i) = nI_P(W_T; U_T|Z_T, T)$$

$$= nI_P(W_T, T; U_T|Z_T) \quad (38)$$

$$= nI_P(W; U|Z). \quad (39)$$

Here, (36) follows since the sequences (U^n, Z^n) are memoryless; (37) follows since $Y^{i-1} - (M, U^{i-1}, Z^{i-1}, Z_{i+1}^n) - U_i$; (38) follows from the fact that T is independent of all the other r.v.'s.

The equivocation of source S^n under the null hypothesis can be bounded as follows.

$$\begin{aligned} H(S^n|M, Y^n, Z^n, H=0) &= \sum_{i=1}^n H(S_i|M, S^{i-1}, Y^n, Z^n, H=0) \\ &\leq \sum_{i=1}^n H(S_i|M, Y^{i-1}, Y_i, Z^{i-1}, Z_i, Z_{i+1}^n, H=0) \\ &= \sum_{i=1}^n H(S_i|W_i, Y_i, Z_i, H=0) \\ &= nH(S_T|W_T, Y_T, Z_T, T, H=0) \\ &= nH_P(S|W, Y, Z), \end{aligned} \quad (40)$$

where $P_{SUYZW} = P_{SUYZ}P_{W|U}$ for some conditional distribution $P_{W|U}$.

Finally, we prove the upper bound on κ . For any encoding function $f^{(n)}$ and decision region $\mathcal{A}_n \subseteq \mathcal{M} \times \mathcal{Y}^n \times \mathcal{Z}^n$ for H_0

such that $\epsilon_n \rightarrow 0$, we have,

$$\begin{aligned} D(P_{MY^n Z^n} \| Q_{MY^n Z^n}) &\geq P_{MY^n Z^n}(\mathcal{A}_n) \log \left(\frac{P_{MY^n Z^n}(\mathcal{A}_n)}{Q_{MY^n Z^n}(\mathcal{A}_n)} \right) + P_{MY^n Z^n}(\mathcal{A}_n^c) \log \left(\frac{P_{MY^n Z^n}(\mathcal{A}_n^c)}{Q_{MY^n Z^n}(\mathcal{A}_n^c)} \right) \\ &\geq -H(\epsilon_n) - (1 - \epsilon_n) \log \left(\beta \left(f^{(n)}, \epsilon_n \right) \right). \end{aligned} \quad (41)$$

Here, (41) follows from the log-sum inequality [37]. Thus,

$$\begin{aligned} \limsup_{n \rightarrow \infty} \frac{-\log(\beta(f^n, 0))}{n} &\leq \limsup_{n \rightarrow \infty} \frac{1}{n} D(P_{MY^n Z^n} \| Q_{MY^n Z^n}) \\ &= \limsup_{n \rightarrow \infty} \frac{1}{n} I_P(M; Y^n | Z^n) \end{aligned} \quad (42)$$

$$= H_P(Y|Z) - \liminf_{n \rightarrow \infty} \frac{1}{n} H_P(Y^n | M, Z^n), \quad (43)$$

where (42) follows since $Q_{MY^n Z^n} = P_{MZ^n} P_{Y^n | Z^n}$. The last term can be single-letterized as follows.

$$\begin{aligned} H_P(Y^n | M, Z^n) &= \sum_{i=1}^n H_P(Y_i | Y^{i-1}, M, Z^n) \\ &= \sum_{i=1}^n H_P(Y_i | Z_i, W_i) \\ &= n H_P(Y_Q | Z_Q, W_Q, Q) \\ &= n H_P(Y | Z, W). \end{aligned} \quad (44)$$

Substituting (44) in (43), we obtain

$$\kappa \leq I_P(Y; W | Z). \quad (45)$$

This completes the proof of the converse and the theorem. ■

Next, we state the result for TACI with a distortion privacy constraint, where the distortion is measured using an arbitrary distortion measure $d(\cdot, \cdot)$. Let $\Delta_{min} := \min_{\phi(u, y, z)} \mathbb{E}_Q [d(S, \phi(U, Y, Z))]$.

Theorem 11. $(R, \kappa, \Delta_0, \Delta_{min}) \in \mathcal{R}_d$ if and only if there exist an auxiliary r.v. W and a deterministic function $\phi : \mathcal{W} \times \mathcal{Y} \times \mathcal{Z} \rightarrow \hat{\mathcal{S}}$ such that

$$R \geq I_P(W; U | Z), \quad (46)$$

$$\kappa \leq I_P(W; Y | Z), \quad (47)$$

$$\Delta_0 \leq \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_P [d(S, \phi(W, Y, Z))], \quad (48)$$

for some P_{SUYZW} as defined in Theorem 10.

Proof: The proof of achievability follows from Theorem 9, similarly to the way Theorem 10 is obtained from Theorem 8. Hence, only differences will be highlighted. Similar to the inequality $\Omega_{min} \leq H_Q(S|U, Y, Z)$ in the proof of Theorem 10, we need to prove the inequality $\Delta_{min} \leq \mathbb{E}_Q [d(S, \phi(W, Y, Z))]$, where $Q_{SUYZW} := Q_{SUYZ} P_{W|U}$ for some conditional

distribution $P_{W|U}$. This can be shown as follows.

$$\begin{aligned}
& \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_Q [d(S, \phi(W, Y, Z))] \\
&= \sum_{u, y, z} Q_{UYZ}(u, y, z) \sum_w P_{W|U}(w|u) \min_{\phi(w, y, z)} \sum_s Q_{S|UYZ}(s|u, y, z) d(s, \phi(w, y, z)) \\
&\geq \sum_{u, y, z} Q_{UYZ}(u, y, z) \sum_{w, s} P_{W|U}(w|u) Q_{S|UYZ}(s|u, y, z) d(s, \phi^*(u, y, z)) \\
&\geq \sum_{u, y, z} Q_{UYZ}(u, y, z) \min_{\phi(u, y, z)} \sum_{w, s} P_{W|U}(w|u) Q_{S|UYZ}(s|u, y, z) d(s, \phi(u, y, z)) \\
&= \sum_{u, y, z} Q_{UYZ}(u, y, z) \min_{\phi(u, y, z)} \sum_s Q_{S|UYZ}(s|u, y, z) d(s, \phi(u, y, z)) \\
&= \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_Q [d(S, \phi(U, Y, Z))] := \Delta_{min},
\end{aligned} \tag{49}$$

where, in (49), $\phi^*(u, y, z)$ is chosen such that

$$\phi^*(u, y, z) := \arg \min_{\phi(w, y, z), w \in \mathcal{W}} \sum_s Q_{S|UYZ}(s|u, y, z) d(s, \phi(w, y, z)).$$

Converse: Let $W = (W_T, T)$ denote the auxiliary r.v. defined in the converse of Theorem 10. Inequalities (46) and (47) follow similarly as obtained in Theorem 10. We prove (48). Defining $\phi(M, Y^n, Z^n, i) := \phi_i(M, Y^n, Z^n)$, we have that,

$$\begin{aligned}
\min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) \mid H = 0 \right] &= \min_{\{\phi(m, y^n, z^n, i)\}_{i=1}^n} \mathbb{E} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi(M, Y^n, Z^n, i)) \mid H = 0 \right] \\
&= \min_{\{\phi(\cdot, \cdot, \cdot, \cdot)\}} \mathbb{E} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi(W_i, Z_i, Y_i, Y_{i+1}^n, i)) \mid H = 0 \right] \\
&\leq \min_{\{\phi(w_i, z_i, y_i, i)\}} \mathbb{E} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi(W_i, Z_i, Y_i, i)) \mid H = 0 \right] \\
&= \min_{\{\phi(\cdot, \cdot, \cdot, \cdot)\}} \mathbb{E} \left[\mathbb{E} [d(S_T, \phi(W_T, Z_T, Y_T, T)) \mid T] \mid H = 0 \right] \\
&= \min_{\{\phi(\cdot, \cdot, \cdot, \cdot)\}} \mathbb{E} [d(S_T, \phi(W_T, Z_T, Y_T, T)) \mid H = 0] \\
&= \min_{\{\phi(w, z, y)\}} \mathbb{E} [d(S, \phi(W, Z, Y)) \mid H = 0].
\end{aligned} \tag{50}$$

In (50), we used the fact that (9) holds for any arbitrary joint distribution on the r.v.'s (S^n, U^n, M, Y^n, Z^n) in place of $\tilde{P}_{S^n U^n M Y^n Z^n}^{(0)}$. Hence, any Δ_0 satisfying (3) satisfies

$$\Delta_0 \leq \min_{\{\phi(w, z, y)\}} \mathbb{E}_P [d(S, \phi(W, Z, Y))].$$

This completes the proof of the converse and the theorem. ■

A more general version of Theorem 10 and Theorem 11 is claimed in [41] as Theorem 7 and Theorem 8, respectively, in which a privacy constraint under the alternate hypothesis is also imposed. However, we have identified a mistake in the converse proof; and hence, a single-letter characterization for this general problem remains open.

To complete the single-letter characterization in Theorem 10 and Theorem 11, we bound the alphabet size of the auxiliary

r.v. W .

Proposition 12. *In Theorem 10 and 11, it suffices to consider auxiliary r.v.'s W such that $|\mathcal{W}| \leq |\mathcal{U}| + 2$.*

Proof: Consider the $|\mathcal{U}| + 2$ functions of $P_{U|W}$,

$$P_U(u_i) = \sum_{w \in \mathcal{W}} P_W(w) P_{U|W}(u_i|w), i = 1, 2, \dots, |\mathcal{U}| - 1, \quad (51)$$

$$H_P(U|W, Z) = \sum_w P_W(w) g_1(P_{U|W}, w), \quad (52)$$

$$H_P(Y|W, Z) = \sum_w P_W(w) g_2(P_{U|W}, w), \quad (53)$$

$$H_P(S|W, Y, Z) = \sum_w P_W(w) g_3(P_{U|W}, w), \quad (54)$$

where,

$$\begin{aligned} g_1(P_{U|W}, w) &= - \sum_{u,z} P_{U|W}(u|w) P_{Z|U}(z|u) \log \left(\frac{P_{U|W}(u|w) P_{Z|U}(z|u)}{\sum_u P_{U|W}(u|w) P_{Z|U}(z|u)} \right), \\ g_2(P_{U|W}, w) &= - \sum_{y,z,u} P_{U|W}(u|w) P_{Y|Z|U}(y, z|u) \log \left(\frac{\sum_u P_{U|W}(u|w) P_{Y|Z|U}(y, z|u)}{\sum_u P_{U|W}(u|w) P_{Z|U}(z|u)} \right), \\ g_3(P_{U|W}, w) &= - \sum_{s,y,z,u} P_{U|W}(u|w) P_{SY|Z|U}(s, y, z|u) \log \left(\frac{\sum_u P_{U|W}(u|w) P_{SY|Z|U}(s, y, z|u)}{\sum_u P_{U|W}(u|w) P_{Y|Z|U}(y, z|u)} \right). \end{aligned}$$

Thus, by the Fenchel-Eggleston-Carathéodory's theorem [42], it is sufficient to have at most $|\mathcal{U}| - 1$ points in the support of W to preserve P_U and three more to preserve $H_P(U|W, Z)$, $H_P(Y|W, Z)$ and $H_P(S|W, Z, Y)$. Noting that $H_P(Y|Z)$ and $H_P(U|Z)$ are automatically preserved since P_U is preserved (and $(Y, Z, S) - U - W$ holds), $|\mathcal{W}| = |\mathcal{U}| + 2$ points are sufficient to preserve the R.H.S. of equations (25)-(27). This completes the proof for the case of \mathcal{R}_e . Similarly, considering the $|\mathcal{U}| + 1$ functions of $P_{W|U}$ given in (51)-(53) and

$$\mathbb{E}_P [d(S, \phi(W, Y, Z))] = \sum_w P_W(w) g_4(w, P_{W|U}), \quad (55)$$

$$\text{where, } g_4(w, P_{W|U}) = \sum_{s,u,y,z} P_{U|W}(u|w) P_{YZS|U}(y, z, s|u) d(s, \phi(w, y, z)), \quad (56)$$

similar result holds also for the case of \mathcal{R}_d . ■

Remark 13. *When $Q_{S|UYZ} = Q_{S|YZ}$, a tight single-letter characterization of \mathcal{R}_e and \mathcal{R}_d exists even if the privacy constraint is active under the alternate hypothesis. This is due to the fact that given Y^n and Z^n , M is independent of S^n under the alternate hypothesis. In this case, $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e$ if and only if there exists an auxiliary r.v. W , such that $(Z, Y, S) - U - W$,*

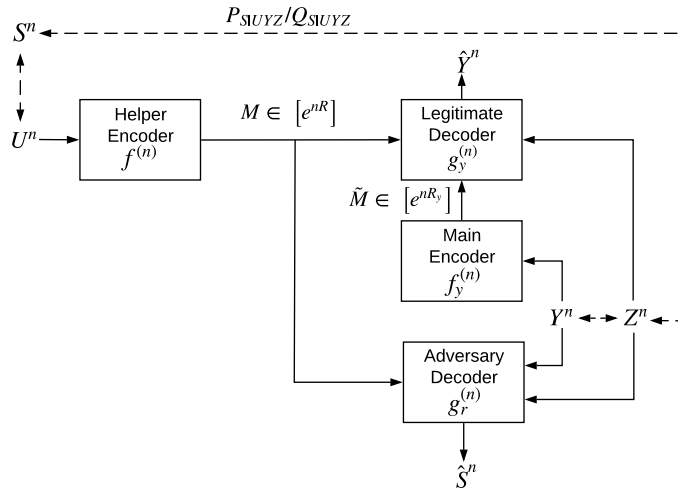


Fig. 2: Source-coding problem in the presence of a helper with a privacy constraint.

and

$$\kappa \leq I_P(W; Y|Z), \quad (57)$$

$$R \geq I_P(W; U|Z), \quad (58)$$

$$\Omega_0 \leq H_P(S|W, Z, Y), \quad (59)$$

$$\Omega_1 \leq H_Q(S|Z, Y), \quad (60)$$

for some P_{SUYZW} as in Theorem 10. Similarly, we have that $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d$ if and only if there exist an auxiliary r.v. W and a deterministic function $\phi: \mathcal{W} \times \mathcal{Y} \times \mathcal{Z} \rightarrow \hat{\mathcal{S}}$ such that (57), (58),

$$\Delta_0 \leq \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_P [d(S, \phi(W, Y, Z))], \quad (61)$$

$$\Delta_1 \leq \min_{\phi(\cdot, \cdot, \cdot)} \mathbb{E}_Q [d(S, \phi(Y, Z))], \quad (62)$$

are satisfied for some P_{SUYZW} as in Theorem 10.

Having established a single-letter characterization of \mathcal{R}_e (resp. \mathcal{R}_d), we briefly mention that this result can also be obtained via the single-letter characterization of the rate-equivocation (resp. rate-distortion) trade-off for an equivalent source-coding problem shown in Fig. 2, which we refer to as the *source-coding problem in the presence of a helper with a privacy constraint*. As it may be of interest on its own, the detailed description of this problem along with a proof of its equivalence to TACI with a privacy constraint is provided in Appendix D.

Theorem 10 (resp. Theorem 11) provide a characterization of \mathcal{R}_e (resp. \mathcal{R}_d) under the condition of vanishing type 1 error probability constraint. Consequently, the converse part of these results are known as *weak converse* results in the context of HT. In the next subsection, we establish the optimal error exponent-privacy trade-off for the special case of zero-rate compression. This trade-off is independent of the type 1 error probability constraint $\epsilon \in (0, 1)$, and hence known as a *strong converse* result.

B. Zero-rate compression

Assume the following zero-rate constraint on the communication between the observer and the detector,

$$\lim_{n \rightarrow \infty} \frac{\log(|\mathcal{M}|)}{n} = 0. \quad (63)$$

Note that (63) does not imply that $|\mathcal{M}| = 0$, i.e., nothing can be transmitted, but that the message set cardinality can grow at most sub-exponentially in n . Such a scenario is motivated practically by low power or low bandwidth constrained applications in which communication is costly. Theorems 14 and 15 stated below provide an optimal single-letter characterization of $\mathcal{R}_d(\epsilon)$ and $\mathcal{R}_e(\epsilon)$ in this case. While the coding schemes in the achievability part of these results are inspired from that in [6], the analysis of privacy achieved at the detector is new. Intuitively, Theorem 15 is based on the fact that at zero-rate, the equivocation of the private part remains essentially unaffected with the knowledge of the message M , and we may borrow results from distributed HT without a privacy constraint problem. On the other hand, to establish Theorem 14, a more detailed analysis of average distortion of S^n at the detector is required, which involves showing that the conditional joint distribution of the private part and the detector's observations given M is close (in terms of the total variation distance) to the unconditional distribution. Lemma 7 serves as a crucial tool for this purpose. We next state the results.

Theorem 14. For $\epsilon \in (0, 1)$, $(0, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$ if and only if it satisfies,

$$\kappa \leq \min_{P_{\tilde{U}\tilde{V}} \in \mathcal{T}_1(P_U, P_V)} D(P_{\tilde{U}\tilde{V}} \| Q_{UV}), \quad (64)$$

$$\Delta_0 \leq \min_{\phi'(\cdot)} \mathbb{E}_P [d(S, \phi'(V))], \quad (65)$$

$$\Delta_1 \leq \min_{\phi'(\cdot)} \mathbb{E}_Q [d(S, \phi'(V))], \quad (66)$$

where $\phi' : \mathcal{V} \rightarrow \hat{S}$ is a deterministic function and

$$\mathcal{T}_1(P_U, P_V) = \{P_{\tilde{U}\tilde{V}} \in \mathcal{T}(\mathcal{U} \times \mathcal{V}) : P_{\tilde{U}} = P_U, P_{\tilde{V}} = P_V\}.$$

Proof: First, we prove that $(0, \kappa, \Delta_0, \Delta_1)$ satisfying (64)-(66) is achievable. While the encoding and decoding scheme is the same as that in [6], we mention it for the sake of completeness.

Encoding: The encoder sends the message $M = 1$ if $U^n \in T_{[P_U]_\delta}^n$, $\delta > 0$, and $M = 0$ otherwise.

Decoding: The detector declares $\hat{H} = 0$ if $M = 1$ and $V^n \in T_{[P_V]_\delta}^n$, $\delta > 0$. Otherwise, $\hat{H} = 1$ is declared.

We analyze the type 1 and type 2 error probabilities for the above scheme as $\delta \rightarrow 0$. First, note by the weak law of large numbers, that, for any $\delta > 0$,

$$\mathbb{P}(U^n \in T_{[P_U]_\delta}^n \cap V^n \in T_{[P_V]_\delta}^n | H = 0) = \mathbb{P}(M = 1 \cap V^n \in T_{[P_V]_\delta}^n | H = 0) \xrightarrow{(n)} 1.$$

Hence, the type 1 error probability tends to zero, asymptotically. The type 2 error can be written as follows.

$$\begin{aligned} \lim_{\delta \rightarrow 0} \beta(f^{(n)}, g^{(n)}) &= \lim_{\delta \rightarrow 0} \mathbb{P}(U^n \in T_{[P_U]_\delta}^n \cap V^n \in T_{[P_V]_\delta}^n | H = 1) \\ &= \lim_{\delta \rightarrow 0} \sum_{\substack{u^n \in T_{[P_U]_\delta}^n, \\ (v^n) \in T_{[P_V]_\delta}^n}} Q_{U^n V^n}(u^n, v^n) \\ &\leq (n+1)^{|U||V|} e^{-n\kappa^*} = e^{-n(\kappa^* - \frac{|U||V|\log(n+1)}{n})}, \end{aligned}$$

where

$$\kappa^* = \min_{P_{\tilde{U}\tilde{V}} \in \mathcal{T}_1(P_U, P_V)} D(P_{\tilde{U}\tilde{V}} \| Q_{UV}).$$

Next, we lower bound the average distortion for S^n achieved by this scheme at the detector. First, note that

$$\mathbb{P}(U^n \in T_{[P_U]_\delta}^n | H = 0) \xrightarrow{(n)} 1, \quad (67)$$

$$\mathbb{P}(U^n \in T_{[P_U]_\delta}^n | H = 1) \xrightarrow{(n)} 1 \text{ if } Q_U = P_U, \quad (68)$$

$$\mathbb{P}(U^n \notin T_{[P_U]_\delta}^n | H = 1) \xrightarrow{(n)} 1 \text{ if } Q_U \neq P_U. \quad (69)$$

This implies that

$$\min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 0 \right] \geq \gamma_{1n} \min_{\{\phi_i(m, v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{P_{S^n V^n | I_U(U^n, \delta)=0}} [d(S_i, \phi_i(1, V^n))] \quad (70)$$

$$\geq \min_{\{\phi'_i(v)\}} \mathbb{E}_P \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi'_i(V_i)) \right] - D_m \gamma_{2n} \quad (71)$$

$$= \min_{\{\phi'(\cdot)\}} \mathbb{E}_P [d(S, \phi'(V))] - D_m \gamma_{2n},$$

for some sequences of positive numbers $\{\gamma_{1n}\}_{n \in \mathbb{Z}^+}$ and $\{\gamma_{2n}\}_{n \in \mathbb{Z}^+}$, such that $\gamma_{1n} \in [0, 1]$, $\forall n \in \mathbb{Z}^+$, $\gamma_{1n} \xrightarrow{(n)} 1$ and $\gamma_{2n} \xrightarrow{(n)} 0$. Here, (70) follows from (67), and (71) follows from (13), Property 2(b) in [43] and the boundedness of the distortion measure, respectively. The average distortion can be bounded similarly under the alternate hypothesis using (68) and (12) when $Q_U = P_U$, and using (69) and (11) when $Q_U \neq P_U$. This completes the proof of the achievability.

We next prove the converse. Note that by the strong converse result in [8], the R.H.S of (64) is an upper bound on the achievable T2EE for all $\epsilon \in (0, 1)$ even without a privacy constraint (hence, also with a privacy constraint). Also,

$$\begin{aligned} \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 0 \right] &\leq \min_{\{\phi'_i(v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{P_{S^n V^n}} [d(S_i, \phi'_i(V^n))] \\ &= \min_{\{\phi'(v)\}} \mathbb{E}_P [d(S, \phi'(V))]. \end{aligned} \quad (72)$$

Here, (72) follows from the fact that the detector can always reconstruct \hat{S}_i as a function of V^n . Similarly,

$$\min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 1 \right] \leq \min_{\{\phi'(v)\}} \mathbb{E}_Q [d(S, \phi'(V))].$$

Hence, any achievable Ω_0 and Ω_1 has to satisfy (65) and (66), respectively. This completes the proof. \blacksquare

The following theorem is the analogous result to Theorem 14 when the privacy measure is equivocation.

Theorem 15. For $\epsilon \in (0, 1)$, $(0, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$ if and only if it satisfies (64) and

$$\Omega_0 \leq H_P(S|V), \quad (73)$$

$$\Omega_1 \leq H_Q(S|V). \quad (74)$$

Proof: For proving the achievability part, the encoding and decoding scheme is the same as in Theorem 14. Note that the following inequality holds for $j = 0, 1$;

$$\frac{1}{n}H(S^n|V^n, H = j) - \frac{1}{n}H(M) \leq \frac{1}{n}H(S^n|M, V^n, H = j) \leq \frac{1}{n}H(S^n|V^n, H = j). \quad (75)$$

Then, (63) and (75) imply that

$$H(S|V, H = j) - \gamma_{3n} \leq \frac{1}{n}H(S^n|M, V^n, H = j) \leq H(S|V, H = j), \quad (76)$$

for some $\gamma_{3n} \xrightarrow{(n)} 0$. Notice that the message M does not play a role in the values of equivocation of S^n at the detector asymptotically. Hence, any T2EE that is achievable under zero-rate compression without a privacy constraint is also achievable under an equivocation constraint. Hence, it follows from the results in [6] and [8] that the R.H.S of (64) is the optimal T2EE achievable for all values of $\epsilon \in (0, 1)$. Moreover, it is clear from (76) that an (Ω_0, Ω_1) pair satisfying (73) and (74) is achievable, and that the R.H.S. of (73) (resp. (74)) is an upper bound for any achievable Ω_0 (resp. Ω_1). This concludes the proof. \blacksquare

In Section II-B, we mentioned that it is possible to achieve a positive T2EE with perfect privacy in our model. Here, we provide an example of TAI with an equivocation privacy constraint under both hypothesis, and show that perfect privacy is possible. Recall that TAI is a special case of TACI, in which, $Z = \text{constant}$, and hence, the null and alternate hypothesis are given by

$$H_0 : (U^n, Y^n) \sim \prod_{i=1}^n P_{UY},$$

$$\text{and } H_1 : (U^n, Y^n) \sim \prod_{i=1}^n P_U P_Y.$$

Example 1. Let $\mathcal{S} = \mathcal{U} = \{0, 1, 2, 3\}$, $\mathcal{Y} = \{0, 1\}$,

$$P_{SU} = 0.125 \cdot \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \quad P_{Y|U} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},$$

$P_{SUY} := P_{SU}P_{Y|U}$ and $Q_{SUY} := P_{SU}P_Y$, where $P_Y = \sum_{u \in \mathcal{U}} P_U(u)P_{Y|U}(y|u)$. Then, we have $H_Q(S|Y) = H_P(S) = H_P(U) = 2$ bits. Also, noting that under the null hypothesis, $Y = U \bmod 2$, $H_P(S|Y) = 2$ bits. It follows from the inner

bound given by equations (28)-(31), and, (34) and (35) that $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$, $\epsilon \in (0, 1)$ if

$$\begin{aligned} R &\geq I_P(W; U), \\ \kappa &\leq I_P(W; Y), \\ \Omega_0 &\leq H_P(S|W, Y), \\ \Omega_1 &\leq H_Q(S|W, Y) = H_Q(S|W), \end{aligned}$$

where $P_{SUYW} := P_{SUY}P_{W|U}$ and $Q_{SUYW} := Q_{SUY}P_{W|U}$ for some conditional distribution $P_{W|U}$. If we set $W := U \bmod 2$, then we have $I_P(U; W) = 1$ bit, $I_P(Y; W) = H_P(Y) = 1$ bit, $H_P(S|W, Y) = H_P(S|Y) = 2$ bits, and $H_Q(S|W) = H_P(S|Y) = 2$ bits. Thus, by revealing only W to the detector, it is possible to achieve a positive T2EE while ensuring maximum privacy under both the null and alternate hypothesis, i.e., the tuple $(1, 1, 2, 2) \in \mathcal{R}_e(\epsilon)$, $\forall \epsilon \in (0, 1)$.

V. A COUNTEREXAMPLE TO THE STRONG CONVERSE

Ahlsvede and Csiszár obtained a strong converse result for the distributed HT problem without a privacy constraint in [5], where they showed that for any positive rate R , the optimal achievable T2EE is independent of the type 1 error probability constraint ϵ . Here, we explore whether a similar result holds in our model, in which, an additional privacy constraint is imposed. We will show through a counterexample that this is not the case in general.

Assume that the joint distribution P_{SUV} is such that $H_P(S|U, V) < H_P(S|V)$. Proving the strong converse amounts to showing that any $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$ for some $\epsilon \in (0, 1)$ also belongs to \mathcal{R}_e . Consider TAI problem with an equivocation privacy constraint, in which, $R \geq H_P(U)$ and $\Omega_1 \leq \Omega_{min}$. Then, from the optimal single-letter characterization of \mathcal{R}_e given in Theorem 10, it follows by taking $W = U$ that $(H_P(U), I_P(V; U), H_P(S|V, U), \Omega_{min}) \in \mathcal{R}_e$. Note that $I_P(V; U)$ is the maximum T2EE achievable for any type 1 error probability constraint $\epsilon \in (0, 1)$, even when U^n is observed directly at the detector. Thus, for vanishing type 1 error probability constraint $\epsilon \rightarrow 0$ and $\kappa = I_P(V; U)$, the term $H_P(S|V, U)$ denotes the maximum achievable equivocation for S^n under the null hypothesis. From the proof of Theorem 10, it follows that the coding scheme for achieving this tuple is as follows.

- 1) Quantize U^n to codewords in $\mathcal{C}_U = \{u^n(j), j \in [1 : 2^{n(H(U)+\delta')}]$, $u^n(j) \in T_{[P_U]_\delta}^n\}$, i.e., if $U^n = u^n \in T_{[P_U]_\delta}^n$, send $M = j$, where j is the index of u^n in \mathcal{C}_U , else, send $M = 0$.
- 2) At the detector, if $M = 0$, declare $\hat{H} = 1$. Else, if $M \neq 0$, declare $\hat{H} = 0$ if $(U^n(M), V^n) \in T_{[P_{UV}]_{\delta'}}^n$, $\delta' > \delta$ and $\hat{H} = 1$, otherwise.

The type 1 error probability of the above scheme tends to zero asymptotically with n . Now, for a fixed $\epsilon^* > 0$, consider a modification of this coding scheme as follows.

- 1) If $U^n = u^n \in T_{[P_U]_\delta}^n$, send $M = j$ with probability $1 - \epsilon^*$, where j is the index of u^n in \mathcal{C}_U , and with probability ϵ^* , send $M = 0$. If $U^n = u^n \notin T_{[P_U]_\delta}^n$, send $M = 0$.
- 2) At the detector, if $M = 0$, declare $\hat{H} = 1$. Else, if $M \neq 0$, declare $\hat{H} = 0$ if $(U^n(M), V^n) \in T_{[P_{UV}]_{\delta'}}^n$, $\delta' > \delta$ and $\hat{H} = 1$, otherwise.

It is easy to see that for this modified coding scheme, the type 1 error probability is asymptotically equal to ϵ^* , while the T2EE remains the same as $I(V;U)$ since the probability of declaring $\hat{H} = 0$ is decreased. Defining $I_U(u^n, \delta) := \mathbb{1}(u^n \notin T_{P_{|U|_\delta}}^n)$, we also have that

$$\begin{aligned} & \frac{1}{n} H(S^n | M, V^n, H = 0) \\ &= (1 - \gamma_n)(1 - \epsilon^*) \frac{1}{n} H(S^n | U^n, V^n, I_U(U^n, \delta) = 0, H = 0) + (1 - \gamma_n) \epsilon^* \frac{1}{n} H(S^n | M = 0, V^n, I_U(U^n, \delta) = 0, H = 0) \\ & \quad + \gamma_n \frac{1}{n} H(S^n | M = 0, V^n, I_U(U^n, \delta) = 1, H = 0) \\ &\geq (1 - \gamma_n)(1 - \epsilon^*) (H_P(S|U, V) - \gamma_n'') + (1 - \gamma_n) \epsilon^* \frac{1}{n} H(S^n | M = 0, V^n, I_U(U^n, \delta) = 0, H = 0) \\ & \quad + \gamma_n \frac{1}{n} H(S^n | M = 0, V^n, I_U(U^n, \delta) = 1, H = 0) \end{aligned} \quad (77)$$

$$\begin{aligned} &> (1 - \gamma_n)(1 - \epsilon^*) (H_P(S|U, V) - \gamma_n'') + (1 - \gamma_n) \epsilon^* \left(H_P(S|U, V) - \frac{\gamma_n'}{n} \right) \\ & \quad + \gamma_n \frac{1}{n} H(S^n | M = 0, V^n, H = 0, I_U(U^n, \delta) = 1) \end{aligned} \quad (78)$$

$$= (1 - \gamma_n)(1 - \epsilon^*) (H_P(S|U, V) - \gamma_n'') + (1 - \gamma_n) \epsilon^* \left(H_P(S|U, V) - \frac{\gamma_n'}{n} \right) + \gamma_n''' \quad (79)$$

$$= (1 - \gamma_n) H_P(S|U, V) - \bar{\gamma}_n, \quad (80)$$

where,

$$\gamma_n := \mathbb{P}(U^n \notin T_{P_{|U|_\delta}}^n) \leq e^{-n\gamma} \xrightarrow{(n)} 0, \quad (81)$$

for some $\gamma > 0$ such that $\gamma \in O(\delta)$, γ_n' is defined in (86) below, $\{\gamma_n''\}_{n \in \mathbb{Z}^+}$ denotes some sequence of positive numbers such that $\gamma_n'' \xrightarrow{(n)} 0$,

$$\gamma_n''' := \frac{\gamma_n}{n} H(S^n | M = 0, V^n, H = 0, I_U(U^n, \delta) = 1) \xrightarrow{(n)} 0, \quad (82)$$

$$\text{and } \bar{\gamma}_n := (1 - \gamma_n)(1 - \epsilon^*) \gamma_n'' + (1 - \gamma_n) \epsilon^* \frac{\gamma_n'}{n} - \gamma_n'''. \quad (83)$$

Equation (77) follows similarly to the proof of Theorem 1 in [44]. Equation (78) is obtained as follows.

$$\begin{aligned} & \frac{1}{n} H(S^n | M = 0, V^n, H = 0, I_U(U^n, \delta) = 0) \\ &\geq \frac{1}{n} H(S^n | V^n, H = 0) - \frac{\gamma_n'}{n} \end{aligned} \quad (84)$$

$$> H_P(S|U, V) - \frac{\gamma_n'}{n} \quad (85)$$

where,

$$\gamma_n' := -2\rho_n^* \log \left(\frac{2\rho_n^*}{|S|^n} \right), \quad (86)$$

$$\rho_n^* := \|P_{S^n V^n | I_U(U^n, \delta)=0, M=0} - P_{S^n V^n}\| = \|P_{S^n V^n | I_U(U^n, \delta)=0} - P_{S^n V^n}\|. \quad (87)$$

Here, (84) is obtained by an application of Lemma 6; and (85) is due to the assumption that $H_P(S|U, V) < H_P(S|V)$.

It follows from Lemma 7 that $\rho_n^* \xrightarrow{(n)} 0$, which in turn implies that

$$\frac{\gamma'_n}{n} \xrightarrow{(n)} 0. \quad (88)$$

From (81), (82) and (88), we have that $\bar{\gamma}_n \xrightarrow{(n)} 0$. Hence, equation (80) implies that $(H_P(U), I_P(V; U), \Omega_0^*, \Omega_{min}) \in \mathcal{R}_e(\epsilon^*)$ for some $\Omega_0^* > H_P(S|U, V)$. Since $(H_P(U), I_P(V; U), \Omega_0^*, \Omega_{min}) \notin \mathcal{R}_e$, this implies that in general, the strong converse does not hold for HT with an equivocation privacy constraint. The same counterexample can be used in a similar manner to show that the strong converse does not hold for HT with an average distortion privacy constraint either.

VI. CONCLUSIONS

We have studied the distributed HT problem with a privacy constraint, with equivocation and average distortion as the measures of privacy. We have established a single-letter inner bound on the rate-error exponent-equivocation and rate-error exponent-distortion trade-offs. We have also obtained the optimal rate-error exponent-equivocation and rate-error exponent-distortion trade-offs for two special cases, when the communication rate over the channel is zero, and for TACI under a privacy constraint. It is interesting to note that the strong converse for distributed HT does not hold when there is an additional privacy constraint in the system. Thus, the problem studied here provides a counterexample to the folklore that *strong converses hold for all memoryless systems*. Extending these results to the case when the communication between the observer and detector takes place over a noisy communication channel is an interesting avenue for future research.

APPENDIX A

PROOF OF LEMMA 7

We will first prove (11). For $\gamma > 0$, define the following sets,

$$\begin{aligned} \mathcal{B}_{0,\gamma}^\delta &:= \{(y^n) \in T_{[P_Y]_\gamma}^n : P_{Y^n}(y^n) \geq P_{Y^n|I_X(X^n,\delta)=0}(y^n)\}, \\ \mathcal{C}_{0,\gamma}^\delta &:= \{(y^n) \in T_{[P_Y]_\gamma}^n : P_{Y^n}(y^n) < P_{Y^n|I_X(X^n,\delta)=0}(y^n)\}, \\ \mathcal{B}_{1,\gamma}^\delta &:= \{(y^n) \in T_{[Q_Y]_\gamma}^n : Q_{Y^n}(y^n) \geq Q_{Y^n|I_X(X^n,\delta)=0}(y^n)\}, \\ \mathcal{C}_{1,\gamma}^\delta &:= \{(y^n) \in T_{[Q_Y]_\gamma}^n : Q_{Y^n}(y^n) < Q_{Y^n|I_X(X^n,\delta)=0}(y^n)\}, \\ \mathcal{B}_{2,\gamma}^\delta &:= \{(y^n) \in T_{[Q_Y]_\gamma}^n : Q_{Y^n}(y^n) \geq Q_{Y^n|I_X(X^n,\delta)=1}(y^n)\}, \\ \mathcal{C}_{2,\gamma}^\delta &:= \{(y^n) \in T_{[Q_Y]_\gamma}^n : Q_{Y^n}(y^n) < Q_{Y^n|I_X(X^n,\delta)=1}(y^n)\}. \end{aligned}$$

Then, we can write

$$\begin{aligned} &\|Q_{Y^n} - Q_{Y^n|I_X(X^n,\delta)=1}\| \\ &= \sum_{y^n} |Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n,\delta)=1}(y^n)| \end{aligned}$$

$$\begin{aligned}
&= \sum_{(y^n) \notin T_{[Q_Y]_\gamma}^n} |Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n)| + \sum_{(y^n) \in T_{[Q_Y]_\gamma}^n} |Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n)| \\
&\leq \sum_{(y^n) \notin T_{[Q_Y]_\gamma}^n} Q_{Y^n}(y^n) + Q_{Y^n|I_X(X^n, \delta)=1}(y^n) + \sum_{(y^n) \in T_{[Q_Y]_\gamma}^n} |Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n)|. \tag{89}
\end{aligned}$$

Next, note that

$$Q_{Y^n|I_X(X^n, \delta)=1}(y^n) = Q_{Y^n}(y^n) \frac{Q_{I_X(X^n, \delta)|Y^n}(1|y^n)}{Q(I_X(X^n, \delta) = 1)} \leq \frac{Q_{Y^n}(y^n)}{Q(I_X(X^n, \delta) = 1)} \leq 2Q_{Y^n}(y^n), \tag{90}$$

for sufficiently large n , since $Q(I_X(X^n, \delta) = 1) \xrightarrow{(n)} 1$. Thus,

$$\sum_{(y^n) \notin T_{[Q_Y]_\gamma}^n} Q_{Y^n}(y^n) + Q_{Y^n|I_X(X^n, \delta)=1}(y^n) \leq 3 \sum_{(y^n) \notin T_{[Q_Y]_\gamma}^n} Q_{Y^n}(y^n) \leq e^{-n\gamma'}. \tag{91}$$

for sufficiently large n for some $\gamma' > 0$. We can bound the term in (89) as follows.

$$\begin{aligned}
&\sum_{(y^n) \in T_{[Q_Y]_\gamma}^n} |Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n)| \\
&= \sum_{(y^n) \in \mathcal{B}_{2, \gamma}^\delta} Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n) + \sum_{(y^n) \in \mathcal{C}_{2, \gamma}^\delta} Q_{Y^n|I_X(X^n, \delta)=1}(y^n) - Q_{Y^n}(y^n) \\
&= \sum_{(y^n) \in \mathcal{B}_{2, \gamma}^\delta} Q_{Y^n}(y^n) - Q_{Y^n|I_X(X^n, \delta)=1}(y^n) + \sum_{(y^n) \in \mathcal{C}_{2, \gamma}^\delta} Q_{Y^n|I_X(X^n, \delta)=1}(y^n) - Q_{Y^n}(y^n) \\
&= \sum_{(y^n) \in \mathcal{B}_{2, \gamma}^\delta} Q_{Y^n}(y^n) \left(1 - \frac{Q_{Y^n|I_X(X^n, \delta)=1}(y^n)}{Q_{Y^n}(y^n)}\right) + \sum_{(y^n) \in \mathcal{C}_{2, \gamma}^\delta} Q_{Y^n}(y^n) \left(\frac{Q_{Y^n|I_X(X^n, \delta)=1}(y^n)}{Q_{Y^n}(y^n)} - 1\right) \\
&= \sum_{(y^n) \in \mathcal{B}_{2, \gamma}^\delta} Q_{Y^n}(y^n) \left(1 - \frac{Q_{I_X(X^n, \delta)|Y^n}(1|y^n)}{Q(I_X(X^n, \delta) = 1)}\right) + \sum_{(y^n) \in \mathcal{C}_{2, \gamma}^\delta} Q_{Y^n}(y^n) \left(\frac{Q_{I_X(X^n, \delta)|Y^n}(1|y^n)}{Q(I_X(X^n, \delta) = 1)} - 1\right) \\
&\leq \sum_{(y^n) \in \mathcal{B}_{2, \gamma}^\delta} Q_{Y^n}(y^n) (1 - Q_{I_X(X^n, \delta)|Y^n}(1|y^n)) + \sum_{(y^n) \in \mathcal{C}_{2, \gamma}^\delta} Q_{Y^n}(y^n) \left(\frac{1}{Q(I_X(X^n, \delta) = 1)} - 1\right). \tag{92}
\end{aligned}$$

Let $P_{\tilde{Y}}$ denote the type of y^n and define

$$E^{(n)}(\delta, \gamma) := \min_{P_{\tilde{Y}} \in T_{[Q_Y]_\gamma}^n} \min_{P_{\tilde{X}} \in T_{[P_X]_\delta}^n} D(P_{\tilde{X}|\tilde{Y}} \| Q_{X|Y} | P_{\tilde{Y}}). \tag{93}$$

Then, for $y^n \in T_{[Q_Y]_\gamma}^n$, arbitrary $\tilde{\gamma} > 0$ and n sufficiently large, we have

$$Q_{I_X(X^n, \delta)|Y^n}(1|y^n) \geq 1 - e^{-n(E^{(n)}(\delta, \gamma) - \tilde{\gamma})}, \tag{94}$$

$$Q(I_X(X^n, \delta) = 1) \geq 1 - e^{-n(D(P_X \| Q_X) - \tilde{\gamma})}. \tag{95}$$

From (89), (91) and (92), it follows that

$$\|Q_{Y^n} - Q_{Y^n|I_X(X^n, \delta)=1}\| \leq e^{-n\gamma'} + e^{-n(E^{(n)}(\delta, \gamma) - \tilde{\gamma})} + e^{-n(D(P_X \| Q_X) - \tilde{\gamma})}. \tag{96}$$

We next show that $E^{(n)}(\delta, \gamma) > 0$ for sufficiently small $\delta > 0$ and $\gamma > 0$. This would imply that the R.H.S of (96) converges to 0 (for $\tilde{\gamma}$ small enough), thus proving (11). We can write,

$$E^{(n)}(\delta, \gamma) \geq \min_{P_{\tilde{Y}} \in T_{[Q_Y]_\gamma}^n} \min_{P_{\tilde{X}} \in T_{[P_X]_\delta}^n} D(P_{\tilde{X}} \| \hat{Q}_X) \quad (97)$$

$$\geq \frac{1}{2 \log 2} * \left[\min_{P_{\tilde{Y}} \in T_{[Q_Y]_\gamma}^n} \min_{P_{\tilde{X}} \in T_{[P_X]_\delta}^n} \|P_{\tilde{X}} - \hat{Q}_X\|^2 \right], \quad (98)$$

where

$$\hat{Q}_X(x) := \sum_y P_{\tilde{Y}}(y) Q_{X|Y}(x|y).$$

Here, (97) follows due to the convexity of KL divergence (98) is due to Pinsker's inequality [37]. We also have from the properties of total variation that,

$$\|P_{\tilde{X}} - \hat{Q}_X\| \geq \|P_X - Q_X\| - \|P_{\tilde{X}} - P_X\| - \|\hat{Q}_X - Q_X\|.$$

For $y^n \in T_{[Q_Y]_\gamma}^n$,

$$\|\hat{Q}_X - Q_X\| \leq \|Q_{X|Y} P_{\tilde{Y}} - Q_{XY}\| \leq \|P_{\tilde{Y}} - Q_Y\| \leq k_1(\gamma),$$

where $k(\gamma) = O(\gamma)$. Also, for $P_{\tilde{X}} \in T_{[P_X]_\delta}^n$,

$$\|P_{\tilde{X}} - P_X\| \leq k_2(\delta),$$

where $k_2(\delta) = O(\delta)$. Hence,

$$E^{(n)}(\delta, \gamma) \geq \frac{1}{2 \log 2} * (\|P_X - Q_X\| - k_1(\gamma) - k_2(\delta))^2.$$

Since $P_X \neq Q_X$, $E^{(n)}(\delta, \gamma) > 0$ for sufficiently small $\gamma > 0$ and $\delta > 0$. This completes the proof of (11).

We next prove (13). Similar to (89) and (90), we have,

$$\begin{aligned} & \|P_{Y^n} - P_{Y^n|I_X(X^n, \delta)=0}\| \\ & \leq \sum_{(y^n) \notin T_{[P_Y]_\gamma}^n} P_{Y^n}(y^n) + P_{Y^n|I_X(X^n, \delta)=0}(y^n) + \sum_{(y^n) \in T_{[P_Y]_\gamma}^n} |P_{Y^n}(y^n) - P_{Y^n|I_X(X^n, \delta)=0}(y^n)|, \end{aligned} \quad (99)$$

and

$$P_{Y^n|I_X(X^n, \delta)=0}(y^n) \leq 2P_{Y^n}(y^n), \quad (100)$$

since $P(I_X(X^n, \delta) = 0) \xrightarrow{(n)} 1$.

Also,

$$\begin{aligned}
& \sum_{(y^n) \in T_{[P_Y]_\gamma}^n} |P_{Y^n}(y^n) - P_{Y^n|I_X(X^n, \delta)=0}(y^n)| \\
&= \sum_{(y^n) \in \mathcal{B}_{0, \gamma}^\delta} P_{Y^n}(y^n) - P_{Y^n|I_X(X^n, \delta)=0}(y^n) + \sum_{(y^n) \in \mathcal{C}_{0, \gamma}^\delta} P_{Y^n|I_X(X^n, \delta)=0}(y^n) - P_{Y^n}(y^n) \\
&\leq \sum_{(y^n) \in \mathcal{B}_{0, \gamma}^\delta} P_{Y^n}(y^n) (1 - P_{I_X(X^n, \delta)|Y^n}(0|y^n)) + \sum_{(y^n) \in \mathcal{C}_{0, \gamma}^\delta} P_{Y^n}(y^n) \left(\frac{1}{P(I_X(X^n, \delta) = 0)} - 1 \right) \leq \tilde{\gamma}_n, \quad (101)
\end{aligned}$$

for some $\tilde{\gamma}_n \xrightarrow{(n)} 0$. Here, (101) follows due to the facts that $P(I_X(X^n, \delta) = 0) \xrightarrow{(n)} 1$, and $P_{I_X(X^n, \delta)|Y^n}(0|y^n) \xrightarrow{(n)} 1$ for $(y^n) \in \mathcal{B}_{0, \gamma}^\delta$ with γ sufficiently small. Thus, from (99), (100) and (101), we can write for some $\gamma' > 0$ that,

$$\|P_{Y^n} - P_{Y^n|I_X(X^n, \delta)=0}\| \leq 3e^{-n\gamma'} + \tilde{\gamma}_n \xrightarrow{(n)} 0.$$

This completes the proof of (13). The proof of (12) is exactly same as (13), with the only difference that the sets $\mathcal{B}_{1, \gamma}^\delta$ and $\mathcal{C}_{1, \gamma}^\delta$ are used in place of $\mathcal{B}_{0, \gamma}^\delta$ and $\mathcal{C}_{0, \gamma}^\delta$, respectively.

APPENDIX B

PROOF OF THEOREM 8

We will present a random coding scheme, and analyze the resulting type 1 and type 2 error probabilities followed by the equivocation of private part S^n at the detector over the ensemble of all randomly generated codebooks. We mention here that unless specified otherwise, the mutual information and entropy terms appearing in the proof below, like for example, $I(U; W)$, $I(U; W|V)$, $H(W|V)$ etc. are computed with respect to the joint distribution induced under the null hypothesis, i.e., $P_{SUVW} = P_{SUV}P_{W|U}$.

Codebook Generation:

Fix a conditional distribution $P_{W|U}$, and positive numbers δ' , δ'' , δ and $\tilde{\delta}$ (arbitrarily small subject to the delta-convention [37] and certain other constraints that will be specified in the course of the proof). Generate $e^{n(I(U; W) + \delta')}$ independent sequences $W^n(j)$, $j \in [e^{n(I(U; W) + \delta')}]$ randomly according to the distribution $\prod_{i=1}^n P_W(w_i)$, where

$$P_W(w) = \sum_{u \in \mathcal{U}} \sum_{w \in \mathcal{W}} P_U(u) P_{W|U}(w|u).$$

Denote this codebook by \mathcal{C}^n .

Encoding: The encoder $f^{(n)} : \mathcal{U}^n \rightarrow [e^{nR}]$ is deterministic with output M , which is chosen as follows. If $I(U; W) + \delta' > R$, the encoder performs uniform random binning on the sequences $W^n(j)$, $j \in [e^{n(I(U; W) + \delta')}]$ in \mathcal{C}^n , i.e., for each codeword in \mathcal{C}^n , it selects an index uniformly at random from the set $[e^{nR}]$. Denote the bin assignment by \mathcal{C}_B^n and the bin index selected for $W^n(j)$ by $f_B(j)$. If the observed sequence U^n is typical, i.e., $U^n \in T_{[P_U]_{\delta''}}^n$, the encoder first looks for a sequence $W^n(J)$ such that $(U^n, W^n(J)) \in T_{[P_{UW}]_\delta}^n$, $\delta > \delta''$. If there exists multiple such codewords, it chooses one of the index J among them uniformly at random and outputs the bin-index $M = f_B(J)$, $M \in [1 : e^{nR}]$ or $M = J$ depending on whether

$I(U; W) + \delta' > R$ or otherwise. If $U^n \notin T_{[P_U]_{\delta''}}^n$ or such an index J does not exist, the encoder outputs the *error* message $M = 0$.

Decoding: If $M = 0$, $\hat{H} = 1$ is declared. Else, given $M \neq 0$ and V^n , the detector looks for a typical sequence $\hat{W}^n = W^n(\hat{L}) \in T_{[P_W]_{\delta}}^n$, $\hat{\delta} = |\mathcal{U}|\delta$ in \mathcal{C}^n such that

$$\hat{L} = \arg \min_{\substack{l: M=f_B(l), \\ W^n(l) \in T_{[P_W]_{\delta}}^n}} H_e(W^n(l)|V^n).$$

If $(\hat{W}^n, V^n) \in T_{[P_{WV}]_{\delta}}^n$, $\tilde{\delta} > \delta$, $\hat{H} = 0$ is declared, else, $\hat{H} = 1$ is declared.

We next analyze the Type 1 and Type 2 error probabilities achieved by the above scheme (in the limit $\delta, \delta', \tilde{\delta} \rightarrow 0$).

Analysis of Type 1 error: A type 1 error occurs only if one of the following events happen.

$$\begin{aligned} \mathcal{E}_{TE} &= \left\{ (U^n, V^n) \notin T_{[P_{UV}]_{\delta}}^n, \bar{\delta} = \frac{\delta''}{|\mathcal{V}|} \right\}, \\ \mathcal{E}_{EE} &= \left\{ \nexists j \in [1 : e^{n(I(U;W)+\delta')}] : (U^n, W^n(j)) \in T_{[P_{UW}]_{\delta}}^n \right\}, \\ \mathcal{E}_{ME} &= \left\{ (V^n, W^n(J)) \notin T_{[P_{VW}]_{\delta}}^n \right\}, \\ \mathcal{E}_{DE} &= \left\{ \exists l \in [1 : e^{n(I(U;W)+\delta')}] , l \neq J : f_B(l) = f_B(J), W^n(l) \in T_{[P_W]_{\delta}}^n, H_e(W^n(l)|V^n) \leq H_e(W^n(J)|V^n) \right\}, \\ \mathcal{E} &= \mathcal{E}_{TE} \cup \mathcal{E}_{EE} \cup \mathcal{E}_{ME} \cup \mathcal{E}_{DE}. \end{aligned}$$

Hence, the Type 1 error can be upper bounded as

$$\alpha(f^{(n)}) := \inf_{g_h^{(n)}} \alpha(f^{(n)}, g_h^{(n)}) \leq \mathbb{P}(\mathcal{E}|H = 0).$$

\mathcal{E}_{TE} tends to 0 asymptotically by the weak law of large numbers. Note that given \mathcal{E}_{TE}^c holds, $U^n \in T_{[P_U]_{\delta''}}^n$ and by the covering lemma [37, Lemma 9.1], it is well known that \mathcal{E}_{EE} tends to 0 doubly exponentially for $\delta > \delta''$ and δ' appropriately chosen. Given $\mathcal{E}_{EE}^c \cap \mathcal{E}_{TE}^c$ holds, it follows from the Markov chain relation $V - U - W$ and the Markov lemma [42], that $\mathbb{P}(\mathcal{E}_{ME})$ tends to zero as $n \rightarrow \infty$ for $\tilde{\delta} > \delta$ (appropriately chosen). Furthermore,

$$\begin{aligned} &\mathbb{P}(\mathcal{E}_{DE} | V^n = v^n, W^n(J) = w^n, \mathcal{E}_{ME}^c \cap \mathcal{E}_{EE}^c \cap \mathcal{E}_{TE}^c) \\ &\leq \sum_{\substack{l=1, \\ l \neq J}}^{2^{n(I(U;W)+\delta')}} \sum_{\substack{\tilde{w}^n \in T_{[P_W]_{\delta}}^n: \\ H_e(\tilde{w}^n|v^n) \leq H_e(w^n|v^n)}} \mathbb{P}(f_B(l) = f_B(J), W^n(l) = \tilde{w}^n | V^n = v^n, W^n(J) = w^n, \mathcal{E}_{ME}^c \cap \mathcal{E}_{EE}^c \cap \mathcal{E}_{TE}^c) \\ &= \sum_{\substack{l=1, \\ l \neq J}}^{2^{n(I(U;W)+\delta')}} \sum_{\substack{\tilde{w}^n \in T_{[P_W]_{\delta}}^n: \\ H_e(\tilde{w}^n|v^n) \leq H_e(w^n|v^n)}} \mathbb{P}(W^n(l) = \tilde{w}^n | V^n = v^n, W^n(J) = w^n, \mathcal{E}_{ME}^c \cap \mathcal{E}_{EE}^c \cap \mathcal{E}_{TE}^c) \frac{1}{2^{nR}} \\ &\leq \sum_{\substack{l=1, \\ l \neq J}}^{2^{n(I(U;W)+\delta')}} \sum_{\substack{\tilde{w}^n \in T_{[P_W]_{\delta}}^n: \\ H_e(\tilde{w}^n|v^n) \leq H_e(w^n|v^n)}} 2^{-nR} 2^{-n(H(W)-\delta_1)} \end{aligned}$$

$$\begin{aligned}
&\leq \sum_{\substack{l=1, \\ l \neq J}}^{2^{n(I(U;W)+\delta')}} (n+1)^{|\mathcal{V}||\mathcal{W}|} 2^{n(H(W|V)+\gamma_1(n))} \cdot 2^{-nR} 2^{-n(H(W)-\delta_1)} \\
&\leq 2^{-n(R-I(U;W|V)-\delta_2^{(n)})},
\end{aligned}$$

where, $\delta_1 = O(\hat{\delta})$, $\gamma_1(n) = |H_e(w^n|v^n) - H(W|V)|$ and $\delta_2^{(n)} = \delta_1 + \frac{1}{n}|\mathcal{V}||\mathcal{W}| \log(n+1) + \delta' + \gamma_1(n) \xrightarrow{(n)} 0$ as $\tilde{\delta}, \delta', \delta \rightarrow 0$. Hence, $\mathbb{P}(\mathcal{E}_{DE})$ tends to zero as $n \rightarrow \infty$ provided that $R > I(U;W|V)$, which in turn implies from the union bound that $\alpha(f^{(n)}) \xrightarrow{(n)} 0$.

Analysis of Type 2 error: A type 2 error occurs only if $V^n \in T_{[P_V]_{\delta'''}}^n$, $\delta''' = |\mathcal{W}|\tilde{\delta}$ and $M \neq 0$, i.e., $U^n \in T_{[P_U]_{\delta''}}^n$ and \mathcal{E}_{EE} does not occur. Hence, we can restrict the type 2 error analysis to only such (U^n, V^n) . Denote the event that a type 2 error happens by \mathcal{D}_0 . Let

$$\mathcal{E}_{T2} = \left\{ U^n \notin T_{[P_U]_{\delta''}}^n \text{ or } V^n \notin T_{[P_V]_{\delta'''}}^n \right\}. \quad (102)$$

The type 2 error probability can be written as

$$\beta(f^{(n)}, \epsilon) = \sum_{(u^n, v^n) \in \mathcal{U}^n \times \mathcal{V}^n} \mathbb{P}(U^n = u^n, V^n = v^n | H = 1) \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, H = 1). \quad (103)$$

Let $\mathcal{E}_{NE} := \mathcal{E}_{EE}^c \cap \mathcal{E}_{T2}^c$. The last term in (103) can be upper bounded as follows.

$$\begin{aligned}
&\mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, H = 1) \\
&= \mathbb{P}(\mathcal{E}_{NE} | U^n = u^n, V^n = v^n, H = 1) \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) \\
&\leq \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1).
\end{aligned}$$

Thus, we have

$$\beta(f^{(n)}, \epsilon) \leq \sum_{(u^n, v^n) \in \mathcal{U}^n \times \mathcal{V}^n} \mathbb{P}(U^n = u^n, V^n = v^n | H = 1) \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1), \quad (104)$$

where,

$$\begin{aligned}
\mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) &= \sum_{j=1}^{e^{n(I(U;W)+\delta')}} \sum_{m=1}^{e^{nR}} \mathbb{P}(J = j, f_B(J) = m | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) \\
&\quad \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = j, f_B(J) = m, \mathcal{E}_{NE}, H = 1).
\end{aligned} \quad (105)$$

By the symmetry of the codebook generation, encoding and decoding procedure, the term $\mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = j, f_B(J) = m, \mathcal{E}_{NE}, H = 1)$ in (105) is independent of the value of J and $f_B(J)$. Hence, w.l.o.g., assuming $J = 1$ and $f_B(J) = 1$, we can write

$$\begin{aligned}
& \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) \\
&= \sum_{j=1}^{e^{n(I(U;W)+\delta')}} \sum_{m=1}^{e^{nR}} \mathbb{P}(J = j, f_B(J) = m | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) \\
&\quad \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \\
&= \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \\
&= \sum_{w^n \in \mathcal{W}^n} \mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \\
&\quad \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}, H = 1). \tag{106}
\end{aligned}$$

Given \mathcal{E}_{NE} holds, \mathcal{D}_0 may occur in two possible ways (i) when an unintended wrong codeword is retrieved from the bin with index M that is jointly typical with V^n and (ii) when the correct codeword is jointly typical with V^n . We refer to the event in case (i) as the *binning error event* \mathcal{E}_{BE} . More specifically,

$$\mathcal{E}_{BE} = \left\{ \exists l \in [1 : e^{n(I(U;W)+\delta')}] , l \neq J, f_B(l) = M, W^n(l) \in T_{[P_W]_\delta}^n, (V^n, W^n(l)) \in T_{[P_{VW}]_\delta}^n \right\}. \tag{107}$$

Define the following events

$$\mathcal{F} = \{U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}\}, \tag{108}$$

$$\mathcal{F}_1 = \{U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}, \mathcal{E}_{BE}^c\}, \tag{109}$$

$$\mathcal{F}_2 = \{U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}, \mathcal{E}_{BE}\}. \tag{110}$$

The last term in (106) can be expressed as follows.

$$\mathbb{P}(\mathcal{D}_0 | \mathcal{F}, H = 1) = \mathbb{P}(\mathcal{E}_{BE}^c | \mathcal{F}, H = 1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_1, H = 1) + \mathbb{P}(\mathcal{E}_{BE} | \mathcal{F}, H = 1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_2, H = 1).$$

For the case $I(U;W) > R$, \mathcal{E}_{BE} happens when a wrong codeword $W^n(l)$, $l \neq J$ is retrieved from the bin with index M by the empirical entropy decoder such that $(W^n(l), V^n) \in T_{[P_{WV}]_\delta}^n$. Let $P_{\tilde{U}\tilde{V}\tilde{W}}$ denote the type of $P_{U^n V^n W^n(J)}$. Note that $P_{\tilde{U}\tilde{W}} \in \mathcal{T}_{[P_{UW}]_\delta}^n$ when \mathcal{E}_{NE} holds. If $H(\tilde{W}|\tilde{V}) < H(W|V)$, there exists a codeword in the bin with index M having empirical entropy strictly less than $H(W|V)$. Hence, the decoded codeword \hat{W}^n is such that $(\hat{W}^n, V^n) \notin T_{[P_{WV}]_\delta}^n$ (asymptotically) since $(\hat{W}^n, V^n) \in T_{[P_{WV}]_\delta}^n$ necessarily implies that $H_e(\hat{W}^n|V^n) := H(P_{\hat{W}^n|V^n} | P_{V^n}) \rightarrow H(W|V)$ as $\delta \rightarrow 0$. Consequently, a Type 2 error can happen under the event \mathcal{E}_{BE} only when $H(\tilde{W}|\tilde{V}) \geq H(W|V)$. The probability of the event \mathcal{E}_{BE} can be upper bounded under this condition as

$$\begin{aligned}
& \mathbb{P}(\mathcal{E}_{BE} | \mathcal{F}, H = 1) \\
& \leq \mathbb{P}\left(\exists l \neq 1, l \in [1 : 2^{n(I(U;W)+\delta')}] : f_B(l) = 1 \text{ and } (W^n(l), v^n) \in T_{[P_{WV}]_\delta}^n \middle| \mathcal{F}\right)
\end{aligned}$$

$$\begin{aligned}
&\leq \sum_{l=2}^{2^{n(I(U;W)+\delta')}} \mathbb{P}\left((W^n(l), v^n) \in T_{[P_{WV}]_{\tilde{\delta}}}^n \mid \mathcal{F}\right) \mathbb{P}\left(f_B(l) = 1 \mid \mathcal{F}_2, (W^n(l), v^n) \in T_{[P_{WV}]_{\tilde{\delta}}}^n\right) \\
&= \sum_{l=2}^{2^{n(I(U;W)+\delta')}} \mathbb{P}\left((W^n(l), v^n) \in T_{[P_{WV}]_{\tilde{\delta}}}^n \mid \mathcal{F}\right) 2^{-nR} \\
&\leq \sum_{l=2}^{2^{n(I(U;W)+\delta')}} \sum_{(\tilde{w}^n, v^n) \in T_{[P_{WV}]_{\tilde{\delta}}}^n} \mathbb{P}(W^n(l) = \tilde{w}^n \mid U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, \mathcal{E}_{CE}^c) 2^{-nR} \tag{111} \\
&\leq \sum_{l=2}^{2^{n(I(U;W)+\delta')}} \sum_{(\tilde{w}^n, v^n) \in T_{[P_{WV}]_{\tilde{\delta}}}^n} 2^{-nR} 2^{-n(H(W)-\delta_1)} \\
&\leq \sum_{\substack{l=1, \\ l \neq J}}^{2^{n(I(U;W)+\delta')}} (n+1)^{|\mathcal{V}||\mathcal{W}|} 2^{n(H(W|V)+\delta_3)} \cdot 2^{-nR} 2^{-n(H(W)-\delta_1)} \\
&\leq 2^{-n(R-I(U;W|V)-\delta_4^{(n)})}, \tag{112}
\end{aligned}$$

where $\delta_4^{(n)} \xrightarrow{(n)} 0$ as $\delta, \delta', \tilde{\delta} \rightarrow 0$. Also, note that, by definition, $\mathbb{P}(\mathcal{D}_0 \mid \mathcal{F}_2) = 1$.

We proceed to analyze the R.H.S of (104) which upper bounds the type 2 error $\beta(f^{(n)}, \epsilon)$, in the limit $n \rightarrow \infty$ and $\delta, \delta', \tilde{\delta} \rightarrow 0$. From (106), it follows that

$$\begin{aligned}
&\lim_{n \rightarrow \infty} \lim_{\delta, \delta', \tilde{\delta} \rightarrow 0} \sum_{u^n, v^n} \mathbb{P}(U^n = u^n, V^n = v^n \mid H = 1) \mathbb{P}(\mathcal{D}_0 \mid U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H = 1) \\
&= \lim_{n \rightarrow \infty} \lim_{\delta, \delta', \tilde{\delta} \rightarrow 0} \sum_{u^n, v^n} \mathbb{P}(U^n = u^n, V^n = v^n \mid H = 1) \\
&\quad \mathbb{P}(\mathcal{D}_0 \mid U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1). \tag{113}
\end{aligned}$$

Similar to that in [13], rewriting the summation in (113) as the sum over the types and sequences within a type, we obtain

$$\begin{aligned}
&\mathbb{P}(\mathcal{D}_0 \mid \mathcal{E}_{NE}, H = 1) \\
&= \sum_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}^n(\mathcal{U} \times \mathcal{V} \times \mathcal{W})}} \sum_{\substack{(u^n, v^n, w^n) \\ \in T_{P_{\tilde{U}\tilde{V}\tilde{W}}}^n}} \left[\mathbb{P}(U^n = u^n, V^n = v^n \mid H = 1) \right. \\
&\quad \left. \mathbb{P}(W^n(1) = w^n \mid U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \mathbb{P}(\mathcal{D}_0 \mid \mathcal{F}, H = 1) \right] \tag{114}
\end{aligned}$$

Since H_1 is the true underlying hypothesis, we have

$$\begin{aligned}
&\mathbb{P}(U^n = u^n, V^n = v^n \mid H = 1) \mathbb{P}(W^n(1) = w^n \mid U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \\
&\leq e^{-n(H(\tilde{U}\tilde{V}) + D(P_{\tilde{U}\tilde{V}} \parallel Q_{UV}) + H(\tilde{W} \mid \tilde{U}) - \frac{1}{n} |\mathcal{U}| |\mathcal{W}| \log(n+1))}. \tag{115}
\end{aligned}$$

where $P_{\tilde{U}\tilde{V}\tilde{W}}$ denotes the type of the sequence (u^n, v^n, w^n) .

With (112) and (115), we have the necessary machinery to analyze (114). First, consider that the event $\mathcal{E}_{NE} \cap \mathcal{E}_{BE}^c$ holds.

In this case,

$$\begin{aligned} \mathbb{P}(\mathcal{D}_0|\mathcal{F}_1, H = 1) &= \mathbb{P}(\mathcal{D}_0|U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}, \mathcal{E}_{BE}^c, H = 1) \\ &= \begin{cases} 1, & \text{if } P_{u^n w^n} \in T_{[UW]_\delta}^n \text{ and } P_{v^n w^n} \in T_{[VW]_\delta}^n, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \quad (116)$$

Thus, the following terms in (114) can be simplified (in the limit $\delta, \tilde{\delta} \rightarrow 0$) as

$$\begin{aligned} &\lim_{n \rightarrow \infty} \lim_{\delta, \tilde{\delta}, \delta' \rightarrow 0} \sum_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}^n(\mathcal{U} \times \mathcal{V} \times \mathcal{W})}} \sum_{(u^n, v^n, w^n) \in T_{P_{\tilde{U}\tilde{V}\tilde{W}}}^n} \left[\mathbb{P}(U^n = u^n, V^n = v^n | H = 1) \mathbb{P}(\mathcal{E}_{BE}^c | \mathcal{F}, H = 1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_1, H = 1) \right. \\ &\quad \left. \mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \right] \\ &\leq \lim_{n \rightarrow \infty} \lim_{\delta, \tilde{\delta}, \delta' \rightarrow 0} \sum_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}^n(\mathcal{U} \times \mathcal{V} \times \mathcal{W})}} \sum_{(u^n, v^n, w^n) \in T_{P_{\tilde{U}\tilde{V}\tilde{W}}}^n} \left[\mathbb{P}(U^n = u^n, V^n = v^n | H = 1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_1, H = 1) \right. \\ &\quad \left. \mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \right] \\ &\leq \lim_{n \rightarrow \infty} (n+1)^{|\mathcal{U}||\mathcal{V}||\mathcal{W}|} \max_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}_1(P_{UW}, P_{VW})}} e^{nH(\tilde{U}\tilde{V}\tilde{W})} e^{-n(H(\tilde{U}\tilde{V}) + D(P_{\tilde{U}\tilde{V}} || Q_{UV}) + H(\tilde{W}|\tilde{U}) - \frac{1}{n}|\mathcal{U}||\mathcal{W}| \log(n+1))} \quad (117) \\ &= \lim_{n \rightarrow \infty} e^{-n\tilde{E}_{1n}}. \end{aligned}$$

where

$$\begin{aligned} \tilde{E}_{1n} &:= \min_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}_1(P_{UW}, P_{VW})}} H(\tilde{U}\tilde{V}) + D(P_{\tilde{U}\tilde{V}} || Q_{UV}) + H(\tilde{W}|\tilde{U}) - H(\tilde{U}\tilde{V}\tilde{W}) \\ &\quad - \frac{1}{n}|\mathcal{U}||\mathcal{V}||\mathcal{W}| \log(n+1) - \frac{1}{n}|\mathcal{U}||\mathcal{W}| \log(n+1) \\ &= \min_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}_1(P_{UW}, P_{VW})}} \sum P_{\tilde{U}\tilde{V}\tilde{W}} \log \left(\frac{P_{\tilde{U}\tilde{V}}}{Q_{UV}} \frac{1}{P_{\tilde{U}\tilde{V}}} \frac{P_{\tilde{U}}}{P_{\tilde{U}\tilde{W}}} P_{\tilde{U}\tilde{V}\tilde{W}} \right) - o(1) \\ &= \min_{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{T}_1(P_{UW}, P_{VW})} D(P_{\tilde{U}\tilde{V}\tilde{W}} || Q_{UVW}) - o(1) \xrightarrow{(n)} E_1(P_{W|U}), \end{aligned} \quad (118)$$

where $Q_{UVW} = Q_{UV}P_{W|U}$. To obtain (117), we used (115) and (116). This results in the term $E_1(P_{W|U})$ in (18).

Next, consider the terms corresponding to the event $\mathcal{E}_{NE} \cap \mathcal{E}_{BE}$ in (114). Note that given the event $\mathcal{F}_2 = \{U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, W^n(1) = w^n, \mathcal{E}_{NE}, \mathcal{E}_{BE}\}$ occurs, $P_{u^n w^n} \in T_{[UW]_\delta}^n$. Also, \mathcal{D}_0 can happen only if $H_e(w^n|v^n) \geq H(W|V) - \gamma_2(\tilde{\delta})$ for some positive function $\gamma_2(\tilde{\delta}) \in O(\tilde{\delta})$ and $P_{v^n} \in T_{[P_V]_{\delta''}}^n$. Using these facts to simplify the terms corresponding to the event $\mathcal{E}_{NE} \cap \mathcal{E}_{BE}$ in (114), we obtain similar to [13],

$$\begin{aligned} &\lim_{n \rightarrow \infty} \lim_{\delta', \delta, \tilde{\delta} \rightarrow 0} \sum_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}^n(\mathcal{U} \times \mathcal{V} \times \mathcal{W})}} \sum_{(u^n, v^n, w^n) \in T_{P_{\tilde{U}\tilde{V}\tilde{W}}}^n} \left[\mathbb{P}(U^n = u^n, V^n = v^n | H = 1) \mathbb{P}(\mathcal{E}_{BE} | \mathcal{F}, H = 1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_2, H = 1) \right. \\ &\quad \left. \mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \right] \\ &= \lim_{n \rightarrow \infty} e^{-n\tilde{E}_{2n}}, \end{aligned} \quad (119)$$

where,

$$\begin{aligned}
E_{2n} &:= \min_{\substack{P_{\tilde{U}\tilde{V}\tilde{W}} \in \\ \mathcal{T}_2(P_{UV}, P_V)}} H(\tilde{U}\tilde{V}) + D(P_{\tilde{U}\tilde{V}}||Q_{UV}) + H(\tilde{W}|\tilde{U}) + R - I(U; W|V) - \frac{1}{n}|\mathcal{U}||\mathcal{V}||\mathcal{W}|\log(n+1) \\
&\quad - \frac{1}{n}|\mathcal{U}||\mathcal{W}|\log(n+1) \\
&\xrightarrow{(n)} E_2(R, P_{W|U}).
\end{aligned} \tag{120}$$

Also, note that \mathcal{E}_{BE} occurs only when $I(U; W) > R$. This completes the analysis of the T2EE.

Next, we lower bound the equivocation of S^n at the adversary as follows. Assume $H = 0$. Let $I_M := \mathbb{1}(M \neq 0)$. Then, we have

$$\begin{aligned}
H(S^n|M, V^n, H = 0) &= H(S^n|M, V^n, I_M, H = 0) \\
&= \mathbb{P}(M = 0|H = 0)H(S^n|M, V^n, I_M = 0, H = 0) + \mathbb{P}(M \neq 0|H = 0)H(S^n|M, V^n, I_M = 1, H = 0) \\
&\geq \gamma_{0n} H(S^n|M, V^n, I_M = 1, H = 0)
\end{aligned} \tag{121}$$

$$\geq \gamma_{0n} H(S^n|W^n(M, M'), V^n, M, I_M = 1, H = 0) \tag{122}$$

$$\geq n(H_P(S|W, V) - \gamma'_{0n}). \tag{123}$$

for some $\gamma_{0n} \xrightarrow{(n)} 1$, $\gamma'_{0n} \xrightarrow{(n)} 0$. Here, (121) follows since under hypothesis H_0 , $\mathbb{P}(\mathcal{E}_{TE} \cup \mathcal{E}_{EE}) \xrightarrow{(n)} 0$; (122) follows since M and X are functions of the codeword $W^n(M, M')$; and (123) follows similarly to the proof of Theorem 1 in [44].

Next, assume that $H = 1$ and $P_U = Q_U$. Let $\mathcal{E}_U = \{U^n \notin T_{[P_U]_{\delta''}}^n\}$. Then, by the weak law of large numbers and covering theorem [42], it follows that

$$\mathbb{P}(\mathcal{E}_U \cup \mathcal{E}_{EE}|H = 1) \xrightarrow{(n)} 0.$$

Consequently, $\mathbb{P}(M \neq 0|H = 1) \xrightarrow{(n)} 1$. Thus, we can write

$$\begin{aligned}
H(S^n|M, V^n, H = 1) &= H(S^n|M, V^n, I_M, H = 1) \\
&= \mathbb{P}(M = 0|H = 1)H(S^n|M, V^n, I_M = 0, H = 1) + \mathbb{P}(M \neq 0|H = 1)H(S^n|M, V^n, I_M = 1, H = 1) \\
&\geq \gamma_{1n} H(S^n|M, V^n, I_M = 1, H = 1)
\end{aligned} \tag{124}$$

$$\geq \gamma_{1n} H(S^n|W^n(M, M'), V^n, M, I_M = 1, H = 1) \tag{125}$$

$$\geq n(H_Q(S|W, V) - \gamma'_{1n}). \tag{126}$$

for some $\gamma_{1n} \xrightarrow{(n)} 1$, $\gamma'_{1n} \xrightarrow{(n)} 0$. Eqn. (126) follows similarly to the proof of Theorem 1 in [44] since $(U^n, W^n(M, M')) \in T_{[P_{UV}]_{\delta}}^n$ and $Q_{S^n V^n|U^n, W^n(M, M')} = \prod_{i=1}^n Q_{SV|U}$.

Now, assume that $H = 1$ and $Q_U \neq P_U$. Then, it follows that for some $0 < \gamma' < D(P_U||Q_U)$,

$$\mathbb{P}(\mathcal{E}_U|H = 1) \geq 1 - e^{-n(D(P_U||Q_U) - \gamma')} := \gamma_{2n} \xrightarrow{(n)} 1. \tag{127}$$

Recalling that $I_U(u^n, \delta'') := \mathbb{1}(u^n \notin T_{[P_U]_{\delta''}}^n)$, we can write

$$\begin{aligned} & H(S^n|M, V^n, H=1) \\ & \geq \gamma_{2n} H(S^n|M, V^n, I_U(U^n, \delta'') = 1, H=1) \\ & = \gamma_{2n} H(S^n|V^n, I_U(U^n, \delta'') = 1, H=1) \end{aligned} \tag{128}$$

$$\geq \gamma_{2n} (H(S^n|V^n, H=1) - \gamma'_{2n}) \tag{129}$$

$$\geq n(H_Q(S|V) - \gamma'_{2n}), \tag{130}$$

for some $\gamma'_{2n} \xrightarrow{(n)} 0$. Eqn. (128) follows since given $I_U(U^n, \delta'') = 1$, $M = 0$. Eqn. (129) follows from the fact that for δ'' small enough,

$$|H(S^n|V^n, H=1) - H(S^n|V^n, I_U(U^n, \delta'') = 1, H=1)| \leq \gamma'_{2n}.$$

which in turn follows from Lemma 6 and 7. Thus, we have shown that $(R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e(\epsilon)$, $\epsilon \in (0, 1)$, provided that (14)-(17) are satisfied, and by the random coding argument, there exists a deterministic codebook that achieves this tuple.

APPENDIX C

PROOF OF THEOREM 9

The generation of the codebook \mathcal{C}^n and the random coding method for analysis is the same as in Theorem 8. However, a stochastic encoder $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$ with output M is used at the observer instead of a deterministic encoder. Again, unless specified otherwise, the mutual information and entropy terms appearing in the proof below, like for example, $I(U; W)$, $I(U; W|V)$, $H(W|V)$ etc. are computed with respect to the joint distribution $P_{SUVW} = P_{SUV}P_{W|U}$. As in Theorem 8, δ' , δ'' , δ and $\tilde{\delta}$ appearing in the proof below denote arbitrarily small positive numbers subject to delta-convention [37] and certain other constraints that will be specified in the course of the proof.

Encoding: For a given codebook \mathcal{C}^n , define a conditional probability distribution

$$P_{E_u}(j|u^n, \mathcal{C}^n) := \frac{\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}{\sum_j \prod_{i=1}^n P_{U|W}(u_i|W_i(j))}. \tag{131}$$

If $I(U; W) + \delta' + \frac{|\mathcal{U}||\mathcal{W}|\log(n+1)}{n} > R$, the encoder performs uniform random binning on the sequences $W^n(j)$, $j \in [e^{n(I(U; W) + \delta')}]$ in \mathcal{C}^n , i.e., for each codeword in \mathcal{C}^n , it selects an index uniformly at random from the set $[e^{n(R - \frac{|\mathcal{U}||\mathcal{W}|\log(n+1)}{n})}]$. Denote the bin assignment by \mathcal{C}_B^n and the bin index selected for $W^n(j)$ by $f_B(j)$. If the observed sequence U^n is typical, i.e., $U^n \in T_{[P_U]_{\delta''}}^n$, then the encoder outputs the message² $M = (T, M')$, $M' = f_B(J)$, $M \in [1 : e^{nR}]$ or $M = (T, J)$ depending on whether $I(U; W) + \delta' + \frac{|\mathcal{U}||\mathcal{W}|\log(n+1)}{n} > R$ or otherwise, where $J \in [e^{n(I(U; W) + \delta')}]$ is selected according to the probability $P_{E_u}(j|u^n, \mathcal{C}^n)$ and T denotes the index of the joint type of $(U^n, W^n(J))$ in the set of types $\mathcal{T}^n(\mathcal{U} \times \mathcal{W})$. If $U^n \notin T_{[P_U]_{\delta''}}^n$, the encoder outputs the *error* message $M = 0$.

²Note that this is valid assignment since the total number of types in $\mathcal{T}^n(\mathcal{U} \times \mathcal{W})$ is upper bounded by $(n+1)^{|\mathcal{U}||\mathcal{W}|}$ [37].

Decoding: If $M = 0$ or $T \notin T_{[P_{UV}]_\delta}^n$, $\hat{H} = 1$ is declared. Else, given $M \neq 0$ and V^n , the detector looks for a typical sequence $\hat{W}^n = W^n(\hat{L}) \in T_{[P_W]_\delta}^n$, $\hat{\delta} = |\mathcal{U}|\delta$ in the codebook such that

$$\hat{L} = \arg \min_{\substack{l: M=f_B(l), \\ W^n(l) \in T_{[P_W]_\delta}^n}} H_e(W^n(l)|V^n).$$

The detector declares $\hat{H} = 0$ if $(\hat{W}^n, V^n) \in T_{[P_{WV}]_\delta}^n$, for $\tilde{\delta} > \delta$, else, $\hat{H} = 1$ is declared.

We next analyze the average of the Type 1 and Type 2 error probabilities achieved by the above scheme (in the limit $\delta, \delta', \tilde{\delta} \rightarrow 0$) over all random codebooks \mathcal{C}^n and \mathcal{C}_B^n .

Analysis of Type 1 error:

The system induced distribution when $H = 0$ is given by

$$\begin{aligned} & \tilde{P}^{(0)}(s^n, u^n, v^n, j, w^n, m, \hat{j}, \hat{w}^n) \\ &= \left[\prod_{i=1}^n P_{SUV}(s_i, u_i, v_i, z_i) \right] P_{E_u}(j|u^n, \mathcal{C}^n) \mathbb{1}(W^n(j) = w^n) \mathbb{1}(f_B(j) = m) P_{ED}(\hat{j}|v^n, m) \\ & \quad \mathbb{1}(W^n(\hat{j}) = \hat{w}^n), \text{ if } u^n \in T_{[P_U]_{\delta''}}^n, \end{aligned} \quad (132)$$

and

$$\tilde{P}^{(0)}(s^n, u^n, v^n, m) = \left[\prod_{i=1}^n P_{SUV}(s_i, u_i, v_i) \right] \mathbb{1}(m = 0), \text{ if } u^n \notin T_{[P_U]_{\delta''}}^n. \quad (133)$$

Consider two auxiliary distribution $\tilde{\Psi}$ and Ψ defined as

$$\begin{aligned} & \tilde{\Psi}^{(0)}(s^n, u^n, v^n, j, w^n, m, \hat{j}, \hat{w}^n) \\ &:= \left[\prod_{i=1}^n P_{SUV}(s_i, u_i, v_i) \right] P_{E_u}(j|u^n, \mathcal{C}^n) \mathbb{1}(W^n(j) = w^n) \mathbb{1}(f_B(j) = m) P_{ED}(\hat{j}|v^n, m) \mathbb{1}(W^n(\hat{j}) = \hat{w}^n), \end{aligned} \quad (134)$$

and

$$\begin{aligned} & \Psi^{(0)}(s^n, u^n, v^n, j, w^n, m, \hat{j}, \hat{w}^n) \\ &:= \frac{1}{e^{n(I(U;W)+\delta')}} \mathbb{1}(W^n(j) = w^n) \left[\prod_{i=1}^n P_{U|W}(u_i|w_i) \right] \left[\prod_{i=1}^n P_{VS|U}(v_i, s_i|u_i) \right] \mathbb{1}(f_B(j) = m) \\ & \quad P_{ED}(\hat{j}|v^n, m) \mathbb{1}(W^n(\hat{j}) = \hat{w}^n). \end{aligned} \quad (135)$$

Note that the distributions $\tilde{P}^{(0)}$, $\Psi^{(0)}$ and $\tilde{\Psi}^{(0)}$ defined are random variables and depend on the codebook realization \mathcal{C}^n and the binning assignment. Also, observe that the stochastic encoder is chosen such that $P_{E_u}(j|u^n, \mathcal{C}^n) = \Psi^{(0)}(j|u^n)$ and hence, the only difference between the joint distribution $\Psi^{(0)}$ and $\tilde{\Psi}^{(0)}$ is the marginal distribution of U^n . By the soft-covering lemma [38] [40], it follows that for some $\gamma_1 > 0$,

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\Psi_{U^n}^{(0)} - \tilde{\Psi}_{U^n}^{(0)}\| | H = 0 \right] \leq \exp(-\gamma_1 n) \xrightarrow{(n)} 0. \quad (136)$$

Hence, from (136) and the properties of total variation, we have

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\Psi^{(0)} - \tilde{\Psi}^{(0)}\| \mid H = 0 \right] \leq \exp(-\gamma_1 n). \quad (137)$$

where the distributions $\Psi^{(0)}$ and $\tilde{\Psi}^{(0)}$ are over the r.v.'s given in (134). Also, note that the only difference between the distributions $\tilde{P}^{(0)}$ and $\tilde{\Psi}^{(0)}$ is P_{E_u} when $u^n \notin T_{[P_U]_{\delta''}}^n$. Since $\mathbb{P}(U^n \notin T_{[P_U]_{\delta''}}^n) \xrightarrow{(n)} 0$, it follows that for some $\{\gamma_{2n}\}_{n \in \mathbb{Z}^+}$ such that $\gamma_{2n} \xrightarrow{(n)} 0$,

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\tilde{P}^{(0)} - \tilde{\Psi}^{(0)}\| \mid H = 0 \right] \leq \gamma_{2n}. \quad (138)$$

Eqns. (137) and (138) together imply that

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\tilde{P}^{(0)} - \Psi^{(0)}\| \mid H = 0 \right] \leq \gamma_{3n} := \gamma_{2n} + \exp(-\gamma_1 n) \xrightarrow{(n)} 0. \quad (139)$$

This means that the system distribution $\tilde{P}^{(0)}$ induced by encoding and decoding operations (when H_0 is the true hypothesis) can be approximated by that under $\Psi^{(0)}$. Let $\tilde{P}^{(1)}$ and $\tilde{\Psi}^{(1)}$ be defined by the R.H.S. of (132), (133) and (134), with P_{SUV} replaced by Q_{SUV} . Let $\Psi^{(1)}$ denote the R.H.S. of (135) with $P_{VS|U}$ replaced by $Q_{VS|U}$. Note that under joint distribution $\Psi^{(l)}$, $l \in \{0, 1\}$,

$$S_i - (W_i(J), V_i) - (M, W^n(J), V^n), \quad i = [1 : n]. \quad (140)$$

Also, since $I(U; W) + \delta' > 0$, by the application of soft-covering lemma,

$$\mathbb{E}_{\mathcal{C}^n} \left[\sum_{i=1}^n \|P_W - \Psi_{W_i}^{(l)}(J)\| \mid H = 0 \right] \leq \exp(-\gamma_4 n) \xrightarrow{(n)} 0, \quad l = 0, 1, \quad (141)$$

for some $\gamma_4 > 0$. From (135), (139) and (141),

$$\mathbb{P}((U^n, W^n(J)) \in T_{[P_{UW}]_{\delta}}^n \mid H = 0) \xrightarrow{(n)} 1. \quad (142)$$

by the weak law of large numbers. A type 1 error occurs only if one of the following events happen.

$$\begin{aligned} \mathcal{E}_{TE} &= \left\{ (U^n, V^n) \notin T_{[P_{UV}]_{\delta}}^n, \bar{\delta} = \frac{\delta''}{|\mathcal{V}|} \right\}, \\ \mathcal{E}_{SE} &= \{T \notin T_{[P_{UW}]_{\delta}}^n\}, \\ \mathcal{E}_{ME} &= \left\{ (V^n, W^n(J)) \notin T_{[P_{VW}]_{\delta}}^n \right\}, \\ \mathcal{E}_{DE} &= \left\{ \exists l \in [1 : e^{n(I(U;W)+\delta')}] , l \neq J : f_B(l) = f_B(J), W^n(l) \in T_{[P_W]_{\delta}}^n, H_e(W^n(l)|V^n) \leq H_e(W^n(J)|V^n) \right\}, \\ \mathcal{E} &= \mathcal{E}_{TE} \cup \mathcal{E}_{SE} \cup \mathcal{E}_{DE}. \end{aligned}$$

Hence, the type 1 error can be upper bounded as

$$\alpha(f^{(n)}) := \inf_{g_h^{(n)}} \alpha(f^{(n)}, g_h^{(n)}) \leq \mathbb{P}(\mathcal{E}|H=0).$$

$\mathbb{P}(\mathcal{E}_{TE})$ tends to 0 asymptotically by the weak law of large numbers. From (142), $\mathbb{P}(\mathcal{E}_{SE}) \xrightarrow{(n)} 0$. Given \mathcal{E}_{SE}^c and \mathcal{E}_{TE}^c holds, it follows from the Markov chain relation $V-U-W$ and the Markov lemma [42], that $\mathbb{P}(\mathcal{E}_{ME})$ tends to zero as $n \rightarrow \infty$ for $\tilde{\delta} > \delta$ (appropriately chosen). Also, similar to that shown in Theorem 8, it follows that

$$\mathbb{P}(\mathcal{E}_{DE} | V^n = v^n, W^n(J) = w^n, \mathcal{E}_{ME}^c \cap \mathcal{E}_{SE}^c \cap \mathcal{E}_{TE}^c, H=0) \leq e^{-n(R-I(U;W|V)-\delta_2^{(n)})}, \quad (143)$$

where $\delta_2^{(n)} \xrightarrow{(n)} 0$ as $\tilde{\delta}, \delta', \delta \rightarrow 0$. Hence, by the union bound, $\alpha(f^{(n)}) \xrightarrow{(n)} 0$ provided $R > I(U;W|V)$ (in the limit $\tilde{\delta}, \delta', \delta \rightarrow 0$).

Analysis of Type 2 error: The analysis is similar to that of Theorem 8. First, note that a type 2 error occurs only if $V^n \in T_{[P_V]_{\delta'''}}^n$, $\delta''' = |\mathcal{W}|\tilde{\delta}$, $M \neq 0$, i.e., $U^n \in T_{[P_U]_{\delta''}}^n$ and $T \in T_{[P_{UW}]_{\delta}}^n$. Hence, we can restrict the type 2 error analysis to only such (U^n, V^n) . Denote the event that a type 2 error happens by \mathcal{D}_0 . The type 2 error probability can be written as

$$\beta(f^{(n)}, \epsilon) = \sum_{(u^n, v^n) \in \mathcal{U}^n \times \mathcal{V}^n} \mathbb{P}(U^n = u^n, V^n = v^n | H=1) \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, H=1). \quad (144)$$

Let $\mathcal{E}_{NE} := \mathcal{E}_{SE}^c \cap \{V^n \in T_{[V]_{\delta'''}}^n\} \cap \{U^n \in T_{[U]_{\delta''}}^n\}$. The last term in (144) can be upper bounded as follows.

$$\begin{aligned} & \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, H=1) \\ &= \mathbb{P}(\mathcal{E}_{NE} | U^n = u^n, V^n = v^n, H=1) \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H=1) \\ &\leq \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H=1). \end{aligned}$$

By averaging over all codebooks \mathcal{C}^n , \mathcal{C}_B^n and using the symmetry of the codebook generation, encoding and decoding procedure, we can write similar to (106) that,

$$\begin{aligned} & \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{NE}, H=1) \\ &= \sum_{w^n \in \mathcal{W}^n} \mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J=1, f_B(J)=1, \mathcal{E}_{NE}, H=1) \\ & \quad \mathbb{P}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J=1, f_B(J)=1, W^n(1) = w^n, \mathcal{E}_{NE}, H=1). \end{aligned} \quad (145)$$

Defining the events \mathcal{E}_{BE} , \mathcal{F} , \mathcal{F}_1 , \mathcal{F}_2 as in eqns. (107), (108), (109), (110), respectively, the last term in (145) can be written as

$$\mathbb{P}(\mathcal{D}_0 | \mathcal{F}, H=1) = \mathbb{P}(\mathcal{E}_{BE}^c | \mathcal{F}, H=1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_1, H=1) + \mathbb{P}(\mathcal{E}_{BE} | \mathcal{F}, H=1) \mathbb{P}(\mathcal{D}_0 | \mathcal{F}_2, H=1). \quad (146)$$

The first term in (145) can upper bounded as

$$\mathbb{P}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_B(J) = 1, \mathcal{E}_{NE}, H = 1) \leq \frac{1}{|T_{P_{\tilde{W}|\tilde{U}}}|} \leq e^{-n(H(\tilde{W}|\tilde{U}) - \frac{1}{n}|\mathcal{U}||\mathcal{W}|\log(n+1))}. \quad (147)$$

To obtain (147), we used the fact that $P_{E_u}(1|u^n, \mathcal{C}^n)$ in (131) is invariant to the joint type $T_{P_{\tilde{U}\tilde{W}}}$ of $(U^n, W^n(1)) = (u^n, w^n)$ (keeping all the other codewords fixed), which in turn implies that given \mathcal{E}_{NE} and the type $P_{\tilde{U}}$ of $U^n = u^n$, each sequence in the conditional type $T_{P_{\tilde{W}|\tilde{U}}}$ is equally likely (in the randomness induced by the random codebook generation and stochastic encoding in (131)) and its probability is upper bounded by $\frac{1}{|T_{P_{\tilde{W}|\tilde{U}}}|}$. The analysis of the other terms in (146) is the same as in Theorem 8 and results in similar factors in the T2EE. Hence, it is omitted. Therefore, by the random coding argument, there exists a sequence of deterministic codebooks $(\mathcal{C}^n, \mathcal{C}_B^n)$ such that it achieves the T2EE given in (15) and satisfies the type 1 error probability constraint ϵ , (142), (139) and (141). Using these codebooks for coding (at the encoder and decoder), we next lower bound the average distortion of S^n at the adversary decoder as follows.

First consider that the null hypothesis holds. Then,

$$\begin{aligned} & \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 0 \right] \\ &= \min_{\{\phi_i(m, v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(0)}} [d(S_i, \phi_i(M, V^n))] \\ &\geq \min_{\{\phi_i(m, v^n)\}} \mathbb{E}_{\Psi^{(0)}} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi_i(M, V^n)) \right] - D_m \gamma_{3n} \end{aligned} \quad (148)$$

$$\geq \min_{\{\phi_i(\cdot, \cdot)\}} \mathbb{E}_{\Psi^{(0)}} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi_i(W_i, V_i)) \right] - D_m \gamma_{3n} \quad (149)$$

$$\geq \min_{\{\phi(\cdot, \cdot)\}} \mathbb{E}_P [d(S, \phi(W, V))] - D_m(\gamma_{3n} + \exp(-\gamma_4 n)). \quad (150)$$

Here, (148) follows from (139) and boundedness of distortion measure; (149) follows from (140); (150) follows from (141) and the fact that $\Psi_{S_i V_i | W_i}^{(0)} = P_{S V | W}^{(0)}$, $i \in [n]$.

Next, consider that the alternate hypothesis holds and that $Q_U = P_U$. Then, from the soft-covering lemma, it again follows that

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\Psi_{U^n}^{(1)} - \tilde{\Psi}_{U^n}^{(1)}\| | H = 1 \right] \leq \exp(-\gamma_1 n) \xrightarrow{(n)} 0. \quad (151)$$

and

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\Psi^{(1)} - \tilde{\Psi}^{(1)}\| | H = 1 \right] \leq \exp(-\gamma_1 n). \quad (152)$$

where the distributions $\Psi^{(1)}$ and $\tilde{\Psi}^{(1)}$ are over the r.v.'s given in (134). Also, note that the only difference between the distributions $\tilde{P}^{(1)}$ and $\tilde{\Psi}^{(1)}$ is P_{E_u} when $u^n \notin T_{[P_U]_{\delta^n}}$. Since $Q_U = P_U$ implies $\mathbb{P}(U^n \notin T_{[P_U]_{\delta^n}} | H = 1) \xrightarrow{(n)} 0$, it follows that

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\tilde{P}^{(1)} - \tilde{\Psi}^{(1)}\| | H = 1 \right] \leq \gamma_{2n} \xrightarrow{(n)} 0. \quad (153)$$

Eqns. (152) and (153) together imply that

$$\mathbb{E}_{\mathcal{C}^n} \left[\|\tilde{P}^{(1)} - \Psi^{(1)}\| | H = 1 \right] \leq \gamma_{3n} := \gamma_{2n} + \exp(-\gamma_1 n) \xrightarrow{(n)} 0. \quad (154)$$

This means that the system distribution $\tilde{P}^{(1)}$ induced by encoding and decoding operations when H_1 is the true hypothesis can be approximated by that under $\Psi^{(1)}$. Then,

$$\begin{aligned} & \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 1 \right] \\ &= \min_{\{\phi_i(m, v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(1)}} [d(S_i, \phi_i(M, V^n))] \\ &\geq \min_{\{\phi_i(m, v^n)\}} \mathbb{E}_{\Psi^{(1)}} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi_i(M, V^n)) \right] - D_m \gamma_{3n} \end{aligned} \quad (155)$$

$$\geq \min_{\{\phi_i(\cdot, \cdot)\}} \mathbb{E}_{\Psi^{(1)}} \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi_i(W_i, V_i)) \right] - D_m \gamma_{3n} \quad (156)$$

$$\geq \min_{\{\phi(\cdot, \cdot)\}} \mathbb{E}_Q [d(S, \phi(W, V))] - D_m (\gamma_{3n} + \exp(-\gamma_4 n)). \quad (157)$$

Now, consider the case $H = 1$ and $Q_U \neq P_U$. Then, it follows that for some $0 < \gamma' < D(P_U || Q_U)$,

$$\mathbb{P}(M = 0 | H = 1) = \mathbb{P}(U^n \notin T_{[P_U]_{\delta''}}^n | H = 1) \geq 1 - e^{-n(D(P_U || Q_U) - \gamma')} := \gamma_{5n} \xrightarrow{(n)} 1.$$

Hence,

$$\begin{aligned} & \min_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = 1 \right] \geq \gamma_{5n} \min_{\{\phi_i(m, v^n)\}_{i=1}^n} \frac{1}{n} \sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(1)}} [d(S_i, \phi_i(0, V^n))] \\ &\geq \min_{\{\phi'_i(v)\}} \mathbb{E}_Q \left[\frac{1}{n} \sum_{i=1}^n d(S_i, \phi'_i(V_i)) \right] - D_m \gamma_{3n} \end{aligned} \quad (158)$$

$$= \min_{\{\phi'(\cdot)\}} \mathbb{E}_Q [d(S, \phi'(V))] - D_m (\gamma_{3n}). \quad (159)$$

Here, (158) follows from Lemma 7. Thus, we have shown that $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$, $\epsilon \in (0, 1)$, provided that (14), (15), (20) and (21) are satisfied. This completes the proof of the theorem.

APPENDIX D

ONE-HELPER LOSSLESS SOURCE CODING PROBLEM WITH A PRIVACY CONSTRAINT

Here, we show the equivalence between the one-helper lossless source coding problem with a privacy constraint shown in Fig. 2 and the HT with a privacy constraint problem. In the one-helper lossless source coding problem with a privacy constraint, the main encoder $f_y^{(n)}$ (resp. helper encoder $f^{(n)}$) sends the message \tilde{M} (resp. M) based on its observation Y^n (resp. U^n) to the legitimate decoder $g_y^{(n)}$ through a noiseless channel with rate constraint R_y (resp. R). The goal of the legitimate decoder $g_y^{(n)}$ is to reconstruct Y^n losslessly using the received indices M and \tilde{M} as well as its side information Z^n . This is a source coding with coded side information problem, studied in [45]. However, in our case, there is an additional sequence S^n and

an adversary decoder $g_r^{(n)}$ which has access to (M, Y^n, Z^n) . The goal is to keep S^n private from the adversary decoder such that (3) (resp. (4)) is satisfied when average distortion (resp. equivocation) is the measure of privacy. Note that the adversary decoder has access to all the information that the legitimate decoder has. Hence, protecting S^n cannot depend on coding techniques that are based on the adversary partially missing data (or having a noisier channel), as is common in many physical layer security related works. We measure the privacy of S^n at the adversary decoder under two cases, namely, when the joint distribution of the r.v.'s (S^n, U^n, Y^n, Z^n) is (i) $\prod_{i=1}^n P_{SUYZ}$ and (ii) $\prod_{i=1}^n Q_{SUYZ}$. The pair of equivocation and average distortion tuples simultaneously achievable in these two cases are of interest.

Definition 16. Given a distortion measure $d : \mathcal{S}^n \times \hat{\mathcal{S}}^n \rightarrow [0, D_m]$, a rate-distortion tuple $(R, R_y, \Delta_0, \Delta_1)$ is achievable if there exists a sequence of encoding functions $f^{(n)} : \mathcal{U}^n \rightarrow [e^{nR}]$, $f_y^{(n)} : \mathcal{Y}^n \rightarrow [e^{nR_y}]$ and decoding functions $g_y^{(n)} : [e^{nR}] \times [e^{nR_y}] \times \mathcal{Z}^n \rightarrow \hat{\mathcal{Y}}^n$ such that

$$\limsup_{n \rightarrow \infty} \mathbb{P}(Y^n \neq \hat{Y}^n) = 0, \quad (160)$$

and (3) are satisfied. Let $\hat{\mathcal{R}}_d$ denote the closure of all achievable $(R, R_y, \Delta_0, \Delta_1)$ tuples.

Definition 17. A rate-equivocation tuple $(R, R_y, \Omega_0, \Omega_1)$ is achievable if there exists a sequence of encoding functions $f^{(n)} : \mathcal{U}^n \rightarrow [e^{nR}]$, $f_y^{(n)} : \mathcal{Y}^n \rightarrow [e^{nR_y}]$ and decoding functions $g_y^{(n)} : [e^{nR}] \times [e^{nR_y}] \times \mathcal{Z}^n \rightarrow \hat{\mathcal{Y}}^n$ such that (4) and (160) are satisfied. Let $\hat{\mathcal{R}}_e$ denote the closure of all achievable $(R, R_y, \Omega_0, \Omega_1)$ tuples.

Let $\mathcal{R}_d^{(n)} = \{(R, \kappa, \Delta_0, \Delta_1)\}$ such that there exists $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$ satisfying

$$\kappa \leq \frac{1}{n} D(P_{MY^n Z^n} \| Q_{MY^n Z^n}) = I(M; Y^n | Z^n), \quad (161)$$

$$\inf_{g_r^{(n)}} \mathbb{E} \left[d(S^n, \hat{S}^n) | H = i \right] \geq \Delta_i, \quad i = 0, 1, \quad (162)$$

$$(Y^n, Z^n, S^n) - U^n - M, \quad M = f^{(n)}(U^n). \quad (163)$$

Similarly, let $\mathcal{R}_e^{(n)} = \{(R, \kappa, \Omega_0, \Omega_1)\}$ such that there exists $f^{(n)} : \mathcal{U}^n \rightarrow [e^{nR}]$ satisfying (161), (163) and

$$\frac{1}{n} H(S^n | M, Y^n, Z^n, H = i) \geq \Omega_i, \quad i = 0, 1. \quad (164)$$

The next theorem provides a multi-letter characterization of $\hat{\mathcal{R}}_d$ and $\hat{\mathcal{R}}_e$.

Theorem 18. Let $\hat{\mathcal{R}}_d^{(n)}$ denote the set of $(R, R_y, \Delta_0, \Delta_1)$ tuples such that (162), (163) and

$$R_y \geq \frac{1}{n} H(Y^n | M, Z^n). \quad (165)$$

are satisfied. Similarly, let $\hat{\mathcal{R}}_e^{(n)}$ denote the set of $(R, R_y, \Omega_0, \Omega_1)$ tuples such that (163), (164) and (165) are satisfied. Then,

$$\hat{\mathcal{R}}_d = \text{cl} \left(\bigcup_n \hat{\mathcal{R}}_d^{(n)} \right), \quad (166)$$

$$\hat{\mathcal{R}}_e = \text{cl} \left(\bigcup_n \hat{\mathcal{R}}_e^{(n)} \right). \quad (167)$$

Proof: We first prove (166). For the achievability part, consider the following scheme.

Encoding: Fix n and $f^{(n)} : \mathcal{U}^n \rightarrow P_{\bar{M}|U^n}$ satisfying (162). For $j \in \mathbb{Z}^+$, upon observing u^{nj} , the helper encoder transmits the super-message $M = (M(1), \dots, M(j))$, where each $M(j) \in [e^{nR}]$ is selected independently according to $P_{\bar{M}|U^n=u^n(j)}$. The main encoder $f_y^{nj} : \mathcal{Y}^{nj} \rightarrow \{1, 2, \dots, e^{njR_y}\}$ performs uniform random binning on Y^{nj} , i.e., for each observed sequence v^{nj} , an index \tilde{M} is chosen uniformly at random from the set $\{1, 2, \dots, e^{njR_y}\}$.

Decoding: On receiving M and \tilde{M} , the legitimate decoder checks for a unique sequence \hat{Y}^{nj} such that $f_y(\hat{Y}^{nj}) = \tilde{M}$ and $(\hat{Y}^{nj}, M, Z^{nj}) \in T_{[Y^n \bar{M} Z^n]_\delta}^j$. If successful, it outputs $g^{(nj)}(M, \tilde{M}, Z^{nj}) = \hat{Y}^{nj}$. Else, an error is declared.

Analysis of the probability of error: The following events may result in an error at the legitimate decoder.

$$\begin{aligned} \mathcal{E}_1 &= \{(Y^{nj}, M, Z^{nj}) \notin T_{[Y^n \bar{M} Z^n]_\delta}^j\}, \\ \mathcal{E}_2 &= \{\exists \tilde{Y}^{nj} \neq Y^{nj}, f_y^{(nj)}(\tilde{Y}^{nj}) = f_y^{(nj)}(Y^{nj}), (\tilde{Y}^{nj}, M, Z^{nj}) \in T_{[Y^n \bar{M} Z^n]_\delta}^j\}. \end{aligned}$$

By the joint typicality lemma [42], $Pr(\mathcal{E}_1) \rightarrow 0$ as $j \rightarrow \infty$. Also,

$$\begin{aligned} \mathbb{P}(\mathcal{E}_2) &= \sum_{y^{nj}, m, z^{nj}} \mathbb{P}(v^{nj}, m, z^{nj}) \mathbb{P}\left(f_y^{nj}(\tilde{Y}^{nj}) = f_y^{nj}(v^{nj}), (\tilde{Y}^{nj}, M, z^{nj}) \in T_{[Y^n \bar{M} Z^n]_\delta}^j\right) \\ &= \sum_{y^{nj}, m, z^{nj}} \mathbb{P}(v^{nj}, m, z^{nj}) \sum_{v^{nj} \in T_{[Y^n \bar{M} Z^n]_\delta}^j} e^{-njR_y} \\ &\leq e^{j(H(Y^n|\bar{M}, Z^n) + \delta)} e^{-njR_y} \\ &= e^{nj\left(\frac{H(Y^n|\bar{M}, Z^n) + \delta}{n} - R_y\right)}. \end{aligned}$$

Hence, $\mathbb{P}(\mathcal{E}_2) \rightarrow 0$ as $j \rightarrow \infty$ if $R_y > H(Y^n|\bar{M}, Z^n) + \delta$. Note that $(Z^n, Y^n) - U^n - \bar{M}$. Also, defining $l(k, n) := k - n\lfloor \frac{k}{n} \rfloor$, we can write,

$$\begin{aligned} &\inf_{g_r^{(k)}} \mathbb{E} \left[d\left(S^k, \hat{S}^k\right) | H = H_i \right] \\ &= \frac{n}{k} \sum_{j=1}^{\lfloor \frac{k}{n} \rfloor} \inf_{g_r^{(n)}} \mathbb{E} \left[d\left(S^n(j), \hat{S}^n(j)\right) | H = H_i \right] + \frac{1}{k} \inf_{g_r^{l(k, n)}} \mathbb{E} \left[d\left(S_{n\lfloor \frac{k}{n} \rfloor + 1}^k, \hat{S}_{n\lfloor \frac{k}{n} \rfloor + 1}^k\right) | H = H_i \right] \\ &\geq \frac{1}{n} \sum_{j=1}^{\lfloor \frac{k}{n} \rfloor} \inf_{g_r^{(n)}} \mathbb{E} \left[d\left(S^n, \hat{S}^n\right) | H = H_i \right] = \frac{\lfloor \frac{k}{n} \rfloor}{n} \Delta_i. \end{aligned} \tag{168}$$

Here, (168) follows since $\left\{M(j), Y_{(j-1)n+1}^{jn}, Z_{(j-1)n+1}^{jn}\right\}_{j \in \mathbb{Z}^+}$ forms an i.i.d. sequence. Taking limit $k \rightarrow \infty$, we obtain

$$\liminf_{k \rightarrow \infty} \inf_{g_r^{(k)}} \mathbb{E} \left[d\left(S^k, \hat{S}^k\right) | H = H_i \right] \geq \Delta_i. \tag{169}$$

Thus, if $(R, R_y, \Delta_0, \Delta_1) \in \hat{\mathcal{R}}_d^{(n)}$, then $(R, R_y, \Delta_0, \Delta_1) \in \hat{\mathcal{R}}_d$. Since $\hat{\mathcal{R}}_d$ is closed by definition, it follows that $cl\left(\hat{\mathcal{R}}_d^{(n)}\right) \subseteq \hat{\mathcal{R}}_d$.

Similarly, for fixed $f^{(n)}$ that satisfies (164), and $M = (M(1), M(2), \dots)$ as before, we have

$$\frac{1}{k}H(S^k|M, Y^k, Z^k, H = H_i) \geq \frac{1}{k} \sum_{j=1}^{\lfloor \frac{k}{n} \rfloor} \frac{1}{n}H(S^n(j)|M(j), Y^n(j), Z^n(j), H = H_i) \geq \frac{\lfloor \frac{k}{n} \rfloor}{k} \Omega_i.$$

Thus,

$$\liminf_{k \rightarrow \infty} \frac{1}{k}H(S^k|M, Y^k, Z^k, H = H_i) \geq \Omega_i, \quad (170)$$

and it follows that $cl(\hat{\mathcal{R}}_e^{(n)}) \subseteq \hat{\mathcal{R}}_e$.

For the converse, we have by Fano's inequality that $H(Y^n|\tilde{M}, M, Z^n) \leq \gamma_n$, where $\gamma_n \rightarrow 0$ as $n \rightarrow \infty$. Hence, we obtain

$$\begin{aligned} nR_y &= \log(|\tilde{\mathcal{M}}|) \geq H(\tilde{M}|M, Z^n) \\ &= H(\tilde{M}|M, Z^n) - H(Y^n|\tilde{M}, M, Z^n) + H(Y^n|\tilde{M}, M, Z^n) \\ &\geq H(Y^n, \tilde{M}|M, Z^n) - \gamma_n \\ &= H(Y^n|M, Z^n) + H(\tilde{M}|Y^n, M, Z^n) - \gamma_n \\ &\geq H(Y^n|M, Z^n) - \gamma_n. \end{aligned}$$

Noting that $(Z^n, Y^n) - U^n - M$, $M \in [e^{nR}]$ and (162) (resp. (164)) holds for any achievable scheme, it follows that $int(\hat{\mathcal{R}}_d) \subseteq \hat{\mathcal{R}}_d^n$ (resp. $int(\hat{\mathcal{R}}_e) \subseteq \hat{\mathcal{R}}_e^n$). Taking closure, this implies that

$$\begin{aligned} \hat{\mathcal{R}}_d &\subseteq cl(\hat{\mathcal{R}}_d^n), \\ \text{and } \hat{\mathcal{R}}_e &\subseteq cl(\hat{\mathcal{R}}_e^n). \end{aligned} \quad (171)$$

This completes the proof of the theorem. ■

Next, we prove an inner and outer bound for $\mathcal{R}_d(\epsilon)$ and $\mathcal{R}_e(\epsilon)$ in terms of multi-letter expressions. The inner bound holds for all $\epsilon \in (0, 1)$, while the outer bound holds only when $\epsilon \rightarrow 0$.

Theorem 19.

$$cl\left(\cup_n \mathcal{R}_d^{(n)}\right) \subseteq \mathcal{R}_d(\epsilon), \forall \epsilon \in (0, 1), \quad (172)$$

$$\mathcal{R}_d \subseteq cl\left(\cup_n \mathcal{R}_d^{(n)}\right), \quad (173)$$

$$cl\left(\cup_n \mathcal{R}_e^{(n)}\right) \subseteq \mathcal{R}_e(\epsilon), \forall \epsilon \in (0, 1), \quad (174)$$

$$\mathcal{R}_e \subseteq cl\left(\cup_n \mathcal{R}_e^{(n)}\right). \quad (175)$$

Proof: For simplicity, denote by V the r.v.'s (Y, Z) . We will prove that for all $\epsilon \in (0, 1)$,

$$\cup_n \mathcal{R}_d^{(n)} \subseteq \mathcal{R}_d(\epsilon), \quad (176)$$

$$\cup_n \mathcal{R}_e^{(n)} \subseteq \mathcal{R}_e(\epsilon). \quad (177)$$

Since $\mathcal{R}_d(\epsilon)$ and $\mathcal{R}_e(\epsilon)$ are closed by definition, this in turn implies that

$$cl\left(\bigcup_n \mathcal{R}_d^{(n)}\right) \subseteq \mathcal{R}_d(\epsilon),$$

$$cl\left(\bigcup_n \mathcal{R}_e^{(n)}\right) \subseteq \mathcal{R}_e(\epsilon).$$

Fix n and an encoding function (possibly stochastic) $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{\bar{M}|U^n}\}$, $\bar{M} = [e^{nR}]$ satisfying (162). Let $M(j)$ denote the encoder output for the j^{th} block of samples $U^n(j)$. Then, the distribution of $M(j)$ is given by

$$P_{M(j)}(m) = \sum_{u^n \in \mathcal{U}^n} P_{U^n(j)}(u^n) P_{\bar{M}|U^n}(m|u^n).$$

Since the sequence $(U^n(1), U^n(2), \dots)$ is i.i.d., so is $(M(1), M(2), \dots)$. The encoder transmits the super-message $M = (M(1), M(2), \dots)$ formed by the concatenation of these sub-messages. Note that $\left\{M(j), V_{(j-1)n+1}^{jn}\right\}_{j \in \mathbb{Z}^+}$ form an infinite sequence of i.i.d. r.v.'s indexed by j . Hence, by the application of Stein's Lemma [5], we have for all $\epsilon \in (0, 1)$ that,

$$\limsup_{j \rightarrow \infty} \frac{\log(\beta(nj, \epsilon))}{nj} \leq \frac{-D(P_{\bar{M}V^n} \| Q_{\bar{M}V^n})}{n}.$$

For $k \geq nj$, $\beta(k, \epsilon) \leq \beta(nj, \epsilon)$. Hence,

$$\limsup_{m \rightarrow \infty} \frac{\log(\beta(m, \epsilon))}{m} \leq \limsup_{j \rightarrow \infty} \frac{\log(\beta(nj, \epsilon))}{nj} \leq \frac{-D(P_{\bar{M}V^n} \| Q_{\bar{M}V^n})}{n}.$$

Note that (163) is satisfied. It can be shown similarly to (169) that

$$\liminf_{k \rightarrow \infty} \inf_{g_r^{(k)}} \mathbb{E} \left[d(S^k, \hat{S}^k) | H = H_i \right] \geq \Delta_i, \quad i = 0, 1,$$

and hence, $(R, \kappa, \Delta_0, \Delta_1)$ satisfying (161), (162) and (163) is achievable. This proves (176).

Also, it can be shown similarly to (170) that

$$\liminf_{k \rightarrow \infty} \frac{1}{k} H(S^k | M, V^k, H = H_i) \geq \Omega_i,$$

which proves (177).

Next, we prove the converse part, i.e.,

$$\mathcal{R}_d \subseteq cl\left(\bigcup_n \mathcal{R}_d^{(n)}\right), \tag{178}$$

$$\mathcal{R}_e \subseteq cl\left(\bigcup_n \mathcal{R}_e^{(n)}\right). \tag{179}$$

We will show that

$$int(\mathcal{R}_d) \subseteq \bigcup_n \mathcal{R}_d^{(n)}, \tag{180}$$

$$int(\mathcal{R}_e) \subseteq \bigcup_n \mathcal{R}_e^{(n)}. \tag{181}$$

This would complete the proof of the converse as (180) and (181) implies (178) and (179), respectively. Let $f^{(n)} : \mathcal{U}^n \rightarrow \{P_{M|U^n}\}$, $\mathcal{M} = [e^{nR}]$ and $\mathcal{A} \subseteq [e^{nR}] \times \mathcal{V}^n$ be an arbitrary encoding function and acceptance region for the detector, such that $\bar{\alpha}(f^{(n)}, g^{(n)}) = P_{MV^n}(\mathcal{A}^c) \leq \epsilon$. Then, we have, by the log-sum inequality [37] that

$$\begin{aligned} D(P_{MV^n} || Q_{MV^n}) &\geq P_{MV^n}(\mathcal{A}^c) \log \left(\frac{P_{MV^n}(\mathcal{A}^c)}{Q_{MV^n}(\mathcal{A}^c)} \right) + P_{MV^n}(\mathcal{A}) \log \left(\frac{P_{MV^n}(\mathcal{A})}{Q_{MV^n}(\mathcal{A})} \right) \\ &= -h \left(\bar{\alpha} \left(f^{(n)}, g^{(n)} \right) \right) - (1 - \epsilon) \log \left(\bar{\beta} \left(f^{(n)}, g^{(n)} \right) \right). \end{aligned}$$

As $0 \leq \alpha(f^{(n)}, g^{(n)}) \leq \epsilon$, $\lim_{\epsilon \rightarrow 0} h(\bar{\alpha}(f^{(n)}, g^{(n)})) \rightarrow 0$. Thus, we have

$$\lim_{\epsilon \rightarrow 0} \frac{1}{n} \log \left(\bar{\beta} \left(f^{(n)}, g^{(n)} \right) \right) \geq \frac{-1}{n} D(P_{MV^n} || Q_{MV^n}). \quad (182)$$

Also, note that (162) and (163) should be satisfied by definition for any achievable $(R, \kappa, \Delta_0, \Delta_1) \in \text{int}(\mathcal{R}_d)$. Similarly, it follows that for any achievable $(R, \kappa, \Omega_0, \Omega_1) \in \text{int}(\mathcal{R}_e)$, (161), (163) and (164) should be satisfied. This completes the proof of the theorem. ■

Corollary 20.

$$\begin{aligned} \mathcal{R}_d &= \text{cl} \left(\cup_n \mathcal{R}_d^{(n)} \right), \\ \mathcal{R}_e &= \text{cl} \left(\cup_n \mathcal{R}_e^{(n)} \right). \end{aligned}$$

Noting that $I(M; Y^n | Z^n) = nH(Y|Z) - H(Y^n | Z^n, M)$, it follows from the definition of \mathcal{R}_e^n (resp. \mathcal{R}_d^n), $\hat{\mathcal{R}}_e^n$ (resp. $\hat{\mathcal{R}}_d^n$), Theorem 18 and Corollary 20 that the following equivalence between \mathcal{R}_e (resp. \mathcal{R}_d) and $\hat{\mathcal{R}}_e$ (resp. $\hat{\mathcal{R}}_d$) holds.

$$\begin{aligned} (R, \kappa, \Omega_0, \Omega_1) \in \mathcal{R}_e &\Leftrightarrow (R, H(Y|Z) - \kappa, \Omega_0, \Omega_1) \in \hat{\mathcal{R}}_e, \\ (R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d &\Leftrightarrow (R, H(Y|Z) - \kappa, \Delta_0, \Delta_1) \in \hat{\mathcal{R}}_d. \end{aligned}$$

REFERENCES

- [1] A. Appari and E. Johnson, "Information security and privacy in healthcare: current state of research," *Int. Journ. Internet and Enterprise Management*, vol. 6, no. 4, pp. 279–314, 2010.
- [2] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *ACM workshop on Privacy in Electronic Society*, Alexandria, VA, USA, Nov. 2005.
- [3] A. Miyazaki and A. Fernandez, "Consumer perceptions of privacy and security risks for online shopping," *Journ. of Consumer Affairs*, vol. 35, no. 1, pp. 27–44, 2001.
- [4] G. Giaconi, D. Gündüz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *arXiv:1802.01166*, To appear in *Signal Proc. magazine*.
- [5] R. Ahlswede and I. Csiszár, "Hypothesis testing with communication constraints," *IEEE Trans. Inf. Theory*, vol. 32, no. 4, pp. 533–542, Jul. 1986.
- [6] T. S. Han, "Hypothesis testing with multiterminal data compression," *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 759–772, Nov. 1987.
- [7] H. Shimokawa, T. S. Han, and S. Amari, "Error bound of hypothesis testing with data compression," in *IEEE Int. Symp. Inf. Theory*, Trondheim, Norway, 1994.

- [8] H. M. H. Shalaby and A. Papamarcou, "Multiterminal detection with zero-rate data compression," *IEEE Trans. Inf. Theory*, vol. 38, no. 2, pp. 254–267, Mar. 1992.
- [9] W. Zhao and L. Lai, "Distributed testing against independence with multiple terminals," in *52nd Annual Allerton Conf.*, IL, USA, Oct. 2014.
- [10] G. Katz, P. Piantanida, and M. Debbah, "Distributed binary detection with lossy data compression," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5207–5227, Aug. 2017.
- [11] M. S. Rahman and A. B. Wagner, "On the optimality of binning for distributed hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 58, no. 10, pp. 6282–6303, Oct. 2012.
- [12] S. Sreekumar and D. Gündüz, "Distributed hypothesis testing over noisy channels," in *IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 2017.
- [13] —, "Distributed hypothesis testing over discrete memoryless channels," *arXiv:1802.07665 [cs.IT]*.
- [14] S. Salehkalaibar, M. Wigger, and R. Timo, "On hypothesis testing against conditional independence with multiple decision centers," *IEEE Trans. Commun.*, Jan. 2018.
- [15] S. Salehkalaibar and M. Wigger, "Distributed hypothesis testing based on unequal-error protection codes," *arXiv:1806.05533*.
- [16] S. Borade, B. Nakiboglu, and L. Zheng, "Unequal error protection: An information-theoretic perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5511–5539, Dec. 2009.
- [17] T. S. Han and K. Kobayashi, "Exponential-type error probabilities for multiterminal hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 2–14, Jan. 1989.
- [18] E. Haim and Y. Kochman, "On binary distributed hypothesis testing," *arXiv:1801.00310*.
- [19] N. Weinberger and Y. Kochman, "On the reliability function of distributed hypothesis testing under optimal detection," *arXiv:1801.03687*.
- [20] R. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Int. Conf. on Data Engineering*, Tokyo, Japan, Apr. 2005.
- [21] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *ACM SIGMOD Int. Conf. on Management of data*, Dallas, USA, May. 2000.
- [22] E. Bertino, "Big data security and privacy," in *IEEE Int. Congress on BigData*, New York, USA, 2015.
- [23] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin, "Protecting data privacy in private information retrieval schemes," *Journ. of Computer and System Sciences*, vol. 60, no. 3, pp. 592–629, Jun. 2000.
- [24] M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis, "Resisting structural re-identification in anonymized social networks," *Journ. Proc. of the VLDB Endowment*, vol. 1, no. 1, pp. 102–114, Aug. 2008.
- [25] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in *IEEE Symp. on Security and Privacy*, Berkeley, USA, 2009.
- [26] J. Liao, L. Sankar, V. Tan, and F. Calmon, "Hypothesis testing under mutual information privacy constraints in the high privacy regime," *IEEE Trans. on Inf. Forensics and Security*, vol. 13, no. 4, pp. 1058 – 1071, Apr. 2018.
- [27] J. Liao, L. Sankar, F. Calmon, and V. Tan, "Hypothesis testing under maximal leakage privacy constraints," in *IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 2017.
- [28] A. Gilani, S. B. Amor, S. Salehkalaibar, and V. Y. F. Tan, "Distributed hypothesis testing with privacy constraints," *arXiv:1806.02015*.
- [29] L. Sweeney, "K-anonymity: a model for protecting privacy," *Int. Journ. on Uncertainty, Fuzziness and Knowledge based Systems*, 2002.
- [30] C. Dwork, "Differential privacy," *Automata, Languages and Programming*, Springer, vol. 4052, pp. 1–12, 2006.
- [31] B. Rassouli and D. Gündüz, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," in *IEEE Inf. Theory Workshop*, Guangzhou, China, 2018.
- [32] I. Wagner and D. Eckhoff, "Technical privacy metrics: a systematic survey," *arXiv:1512.00327v1 [cs.CR]*.
- [33] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Medard, "From the information bottleneck to the privacy funnel," in *IEEE Inf. Theory Workshop*, Hobart, Australia, Nov. 2014.
- [34] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. Inf. Theory*, vol. 34, no. 4, pp. 835–842, Jul. 1988.
- [35] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in *Annual Conf. on Inf. Science and Systems*, Princeton, USA, Mar. 2016.
- [36] Z. Li, T. Oechtering, and D. Gündüz, "Smart meter privacy based on adversarial hypothesis testing," in *IEEE Int. Symp. Inf. Theory*, Aachen, Germany, Jun. 2017.
- [37] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.
- [38] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 163–179, Mar. 1975.

- [39] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 752–772, May. 1993.
- [40] P. Cuff, "Distributed channel synthesis," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7071–7096, Nov. 2013.
- [41] S. Sreekumar, D. Gündüz, and A. Cohen, "Distributed hypothesis testing under privacy constraints," in *IEEE Inf. Theory Workshop*, Guangzhou, China, Nov. 2018.
- [42] A. E. Gamal and Y. H. Kim, *Network Information theory*. Cambridge University Press, 2011.
- [43] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, Dec. 2014.
- [44] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, Jun. 2013.
- [45] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, Nov. 1975.