entropy

MDPI

Article

Privacy-Aware Distributed Hypothesis Testing †

Sreejith Sreekumar [1,*], Asaf Cohen [2] and Deniz Gündüz [3]

[1] Department of Electrical and Computer Engineering, Cornell University, Ithaca, NY 14850, USA
[2] The School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel; coasaf@bgu.ac.il
[3] Department of Electrical and Electronic Engineering, Imperial College London, London SW72AZ, UK; d.gunduz@imperial.ac.uk
* Correspondence: sreejithsreekumar@cornell.edu
† This paper is an extended version of our paper published in Proceedings of IEEE Information TheoryWorkshop (ITW), Guangzhou, 2018.

Received: 1 May2020; Accepted: 12 June 2020; Published: 16 June 2020

Abstract: A distributed binary hypothesis testing (HT) 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 II error exponent of the test for a given type I 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 under a causal disclosure assumption as possible measures of privacy, the trade-off between the communication rate from the observer to the detector, the type II error exponent, and privacy is studied. For the general HT 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 counter-example where the strong converse which holds for distributed HT 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 I error probability constraint.

Keywords: Hypothesis testing; privacy; testing against conditional independence; error exponent; equivocation; distortion; causal disclosure

1. 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 the users ensure a desired level of privacy for the sensitive information revealed, while maximizing the utility subject to this constraint.

In many distributed learning or distributed decision-making 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.

There are several practical scenarios where the above-mentioned trade-off arises. For example, consider the issue of consumer privacy in the context of online shopping. A consumer would like to share some information about his/her shopping behavior, e.g., shopping history and preferences, with the shopping portal 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 a hypothesis 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. Yet another relevant example is the issue of user privacy in the context of wearable Internet of Things (IoT) devices such as smart watches and fitness trackers, which collect information on routine daily activities, and often have a third-party cloud interface.

In this paper, we study distributed HT (DHT) 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 II error probability, known as the type II error exponent (or error exponent henceforth), for a given constraint on the type I 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, error exponent 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.

1.1. Background

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 error exponent and a *strong converse* result which states that the optimal error exponent is independent of the constraint on the type I error probability. Exact single-letter characterization of the optimal error exponent

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 [6,7]. Strong converse is studied in the context of complete data compression and zero-rate compression in [6,8], 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 error exponent 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 error exponent 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 error exponent 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 error exponent 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. The general HT version of this problem over a noisy broadcast channel and DHT over a multiple access channel is explored in [15]. While all the above works consider the asymmetric objective of maximizing the error exponent under a constraint on the type I error probability, the trade-off between the exponential rate of decay of both the type I and type II error probabilities are considered in [16–18].

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 deal with the protection or violation of data privacy in different contexts, e.g., see [19–24]. More relevant for our work, HT under mutual information and maximal leakage privacy constraints have been studied in [25,26], respectively, where the observer 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 error exponent while satisfying the privacy constraint is analyzed. Recently, a distributed version of this problem has been studied in [27], where the observer applies a privacy mechanism to its observed data prior to further coding for compression, and 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 [25–27], we study *DHT with a privacy constraint*, but without considering a separate privacy mechanism at the observer. In Section 2, we will further discuss the differences between the system model considered here and that of [27].

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 (e.g., using wiretap codes). However, in data privacy problems, the sensitive data is to be protected from the same legitimate party that receives the messages and provides the utility; and hence, the above-mentioned techniques for guaranteeing data security are not applicable. Another model frequently used in the context of information-theoretic security assumes the availability of different side information at the legitimate receiver and the eavesdropper [28,29]. A DHT problem with security constraints formulated along these lines is studied in [30], where the authors propose an inner bound on the rate-error exponent-equivocation trade-off. While our model is related to

that in [30] when the side information at the detector and eavesdropper coincide, there are some important differences which will be highlighted in Section 2.3.

Many different privacy measures have been considered in the literature to quantify the amount of private information leakage, such as k-anonymity [31], differential privacy (DP) [32], mutual information leakage [33–35], maximal leakage [36], and total variation distance [37] to count a few; see [38] 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 in the information-theoretic studies of privacy. 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 [34]. It is also shown in [33] that a differentially private scheme is not necessarily private when the information leakage is measured by mutual information. This is done by constructing an example that is differentially private, yet the mutual information leakage is arbitrarily high. Mutual information-based measures have also been used in cryptographic security studies. For example, the notion of semantic security defined in [39] is shown to be equivalent to a measure based on mutual information in [40].

A rate-distortion approach to privacy is first explored by Yamamoto in [41] 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. Recently, there have been several works that have used distortion as a security or privacy metric in several different contexts, such as side-information privacy in discriminatory lossy source coding [42] and rate-distortion theory of secrecy systems [43,44]. More specifically, in [43], the distortion-based security measure is analyzed under a *causal disclosure assumption*, in which the data samples to be protected are causally revealed to the eavesdropper (excluding the current sample), yet the average distortion over the entire block has to satisfy a desired lower bound. This assumption ensures that distortion as a secrecy measure is more *robust* (see ([43], Section I-A)), and could in practice model scenarios in which the sensitive data to be protected is eventually available to the eavesdropper with some delay, but the protection of the current data sample is important. In this paper, we will consider both equivocation and average distortion under a causal disclosure assumption as measures of privacy. In [45], error exponent of a HT adversary is considered to be a privacy measure. This can be considered to be the opposite setting to ours, in the sense that while the goal here is to increase the error exponent under a privacy leakage constraint, the goal in [45] is to reduce the error exponent under a constraint on possible transformations that can be applied on the data.

It is instructive to compare the privacy measures considered in this paper with DP. Towards this, note that average distortion and equivocation (see Definitions 1 and 2) are "average case" privacy measures, while DP is a "worst case" measure that focuses on the statistical indistinguishability of neighboring datasets that differ in just one entry. Considering this aspect, it may appear that these privacy measures are unrelated. However, as shown in [46], there is an interesting connection between them. More specifically, the maximum conditional mutual information leakage between the revealed data Y and an entry in the dataset X_i given all the other $n-1$ entries $X^{-i} = X^n \setminus \{X_i\}$, i.e., $I(Y; X_i|X^{-i})$, is sandwiched between the so-called ϵ- DP and (ϵ, δ)-DP in terms of the strength of the privacy measure, where the maximization is over all distributions P_{X^n} on X^n and entries $i \in [1:n]$ ([46], Theorem 1). This implies that as a privacy measure, equivocation (equivalent to mutual information leakage) is weaker than ϵ- DP, and stronger than (ϵ, δ)-DP, at least for some probability distributions on the data. On the other hand, equivocation and average distortion are relatively well-behaved privacy measures compared to DP, and often result in clean and exact computable characterizations of the optimal trade-off for the problem at hand. Moreover, as already shown in [39,40,47,48], the trade-off resulting from "average" constraints turns out to be the

same as that with more stricter constraints in many interesting cases. Hence, it is of interest to consider such average case privacy measures as a starting point for further investigation with stricter measures.

DP has been used extensively in privacy studies including those that involve learning and HT [49–59]. More relevant to the distributed HT problem at hand is the local differentially private model employed in [49–51,56], in which, depending on the privacy requirement, a certain amount of random noise is injected into the user's data before further processing, while the utility is maximized subject to this constraint. Nevertheless, there are key differences between these models and ours. For example, in [49], the goal is to learn from differentially private "examples", the underlying "concept" (model that maps examples to "labels") such that the error probability in predicting the label for future examples is minimized, irrespective of the statistics of the examples. Hence, the utility in [49] is to learn an unknown model accurately, whereas our objective is to test between two known probability distributions. Furthermore, in our setting (unlike [49–51,56]), there is an additional requirement to satisfy in terms of the communication rate. These differences perhaps also make DP less suitable as a privacy measure in our model relative to equivocation and average distortion. On one hand, imposing a DP measure in our setting may be overly restrictive since there are only two probability distributions involved and DP is tailored for situations where the statistics of the underlying data is unknown. On the other hand, DP is also more unwieldy to analyze under a rate constraint compared to mutual information or average distortion.

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 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 corporations. 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 fundamental and challenging research problem.

1.2. Main Contributions

The main contributions of this work are as follows.

1. In Section 3, Theorem 1 (resp. Theorem 2), we establish a single-letter inner bound on the rate-error exponent-equivocation (resp. rate-error exponent-distortion) trade-off for DHT with a privacy constraint. The distortion and equivocation privacy constraints we consider, which is given in (6) and (7), respectively, are slightly stronger than what is usually considered in the literature (stated in (8) and (9), respectively).
2. Exact characterizations are obtained for some important special cases in Section 4. More specifically, a single-letter characterization of the optimal rate-error exponent-equivocation (resp. rate-error exponent-distortion) trade-off is established for:

   (a) TACI with a privacy constraint (for vanishing type I error probability constraint) in Section 4.1, Proposition 1 (resp. Proposition 2),
   (b) DHT with a privacy constraint for zero-rate compression in Section 4.2, Proposition 4 (resp. Proposition 3).

   Since the optimal trade-offs in Propositions 3 and 4 are independent of the constraint on the type I error probability, they are strong converse results in the context of HT.
3. Finally, in Section 5, we provide a counter-example showing that for a positive rate $R > 0$, the strong converse result does not hold in general for TAI with a privacy constraint.

1.3. Organization

The organization of the paper is as follows. Basic notations are introduced in Section 2.1. The problem formulation and associated definitions are given in Section 2.2. Main results are presented in Section 3 to Section 5. The proofs of the results are presented either in the Appendix or immediately after the statement of the result. Finally, Section 6 concludes the paper with some open problems for future research.

2. Preliminaries

2.1. Notations

$\mathbb{N}$, $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ stand for the set of natural numbers, real numbers and non-negative real numbers, respectively. For $a \in \mathbb{R}_{\geq 0}$, $[a] := \{i \in \mathbb{N},\ i \leq a\}$ and for $a \in \mathbb{R}$, $a^+ := \max\{0, a\}$ (:= represents equality by definition). Calligraphic letters, e.g., $\mathcal{A}$, denotes sets, while $|\mathcal{A}|$ and $\mathcal{A}^c$ denotes its cardinality and complement, respectively. $\mathbb{1}(\cdot)$ denotes the indicator function, while $O(\cdot)$, $o(\cdot)$ and $\Omega(\cdot)$ stands for the standard asymptotic notations of Big-O, Little-O and Big-Ω, respectively. For a real sequence $\{a_n\}_{n\in\mathbb{N}}$ and $b \in \mathbb{R}$, $a_n \xrightarrow{(n)} b$ represents $\lim_{n\to\infty} a_n = b$. Similar notations apply for asymptotic inequalities, e.g., $a_n \overset{(n)}{\geq} b$, means that $\lim_{n\to\infty} a_n \geq b$. Throughout this paper, the base of the logarithms is taken to be e, and whenever the range of the summation is not specified, it means summation over the entire support, e.g., $\sum_u$ denotes $\sum_{u\in\mathcal{U}}$.

All the random variables (r.v.'s) considered in this paper are discrete with finite support unless specified otherwise. We denote r.v.'s, their realizations and support by upper case, lower case and calligraphic letters (e.g., X, x and $\mathcal{X}$), respectively. The joint probability distribution of r.v.'s X and Y is denoted by P_{XY}, while their marginals are denoted by P_X and P_Y. The set of all probability distributions with support $\mathcal{X}$ and $\mathcal{X}\times\mathcal{Y}$ are represented by $\mathcal{P}(\mathcal{X})$ and $\mathcal{P}(\mathcal{X}\times\mathcal{Y})$, respectively. For $j, i \in \mathbb{N}$, the random vector $(X_i, \ldots, X_j)$, $j \geq i$, is denoted by X_i^j, while X^j stands for $(X_1, \ldots, X_j)$. Similar notation holds for the vector of realizations. $X - Y - Z$ denotes a Markov chain relation between the r.v.'s X, Y and Z. $\mathbb{P}_P(\mathcal{E})$ denotes the probability of event $\mathcal{E}$ with respect to the probability measure induced by distribution P, and $\mathbb{E}_P[\cdot]$ denotes the corresponding expectation. The subscript P is omitted when the distribution involved is clear from the context. For two probability distributions P and Q defined on a common support, $P << Q$ denotes that P is absolutely continuous with respect to Q.

Following the notation in [60], for $P_X \in \mathcal{P}(\mathcal{X})$ and $\delta \geq 0$, the P_X-typical set is

$$\mathcal{T}^n_{[P_X]_\delta} := \left\{ x^n \in \mathcal{X}^n : \left| P_X(x') - \frac{1}{n}\sum_{i=1}^n \mathbb{1}(x_i = x') \right| \leq \delta,\ \forall\, x' \in \mathcal{X} \right\},$$

and the P_X-type class (set of sequences of type or empirical distribution P_X) is $\mathcal{T}^n_{P_X} := \mathcal{T}^n_{[P_X]_0}$. The set of all possible types of sequences of length n over an alphabet $\mathcal{X}^n$ and the set of types in $\mathcal{T}^n_{[P_X]_\delta}$ are denoted by $\mathcal{P}^n(\mathcal{X})$ and $\mathcal{P}_n\left(\mathcal{T}^n_{[P_X]_\delta}\right)$, respectively. Similar notations apply for pairs and larger combinations of r.v.'s, e.g., $\mathcal{T}^n_{[P_{XY}]_\delta}$, $\mathcal{T}^n_{P_{XY}}$, $\mathcal{P}^n(\mathcal{X}\times\mathcal{Y})$ and $\mathcal{P}_n\left(\mathcal{T}^n_{[P_{XY}]_\delta}\right)$. The conditional $P_{Y|X}$ type class of a sequence $x^n \in \mathcal{X}^n$ is

$$\mathcal{T}^n_{P_{Y|X}}(x^n) := \{y^n : (x^n, y^n) \in \mathcal{T}^n_{P_{XY}}\}. \tag{1}$$

The standard information-theoretic quantities like 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}, are denoted by $D(P_X||Q_X)$, $H_{P_X}(X)$, $H_{P_{XY}}(X|Y)$ and $I_{P_{XY}}(X;Y)$, respectively. When the distribution of the r.v.'s involved are clear

from the context, the last three quantities are denoted simply by $H(X)$, $H(X|Y)$ and $I(X;Y)$, respectively. Given realizations $X^n = x^n$ and $Y^n = y^n$, $H_e(x^n|y^n)$ denotes the conditional empirical entropy given by

$$H_e(y^n|x^n) := H_{P_{\tilde{X}\tilde{Y}}}(\tilde{Y}|\tilde{X}), \tag{2}$$

where $P_{\tilde{X}\tilde{Y}}$ denotes the joint type of (x^n, y^n). Finally, the total variation between probability distributions P_X and Q_X defined on the same support $\mathcal{X}$ is

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

2.2. Problem Formulation

Consider the HT setup illustrated in Figure 1, where (U^n, V^n, S^n) denote n independent and identically distributed (i.i.d.) copies of triplet of r.v.'s (U, V, S). The observer observes U^n and sends the message index M to the detector over an error-free channel, where $M \sim f_n(\cdot|U^n)$ and $f_n : \mathcal{U}^n \to \mathcal{P}(\mathcal{M})$, $\mathcal{M} = [e^{nR}]$. Given its own observation V^n, the detector performs a HT on the joint distribution 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 and $\hat{H}$ denote the r.v.'s corresponding to the true hypothesis and the output of the HT, respectively, with support $\mathcal{H} = \hat{\mathcal{H}} = \{0, 1\}$, where 0 denotes the null hypothesis and 1 the alternate hypothesis. Let $g_n : \mathcal{M} \times \mathcal{V}^n \to \mathcal{P}(\hat{\mathcal{H}})$ denote the decision rule at the detector, which outputs $\hat{H} \sim g_n(M, V^n)$. Then, the type I and type II error probabilities achieved by a (f_n, g_n) pair are given by

$$\alpha_n (f_n, g_n) := \mathbb{P}(\hat{H} = 1|H = 0) = P_{\hat{H}}(1),$$

and

$$\beta_n (f_n, g_n) := \mathbb{P}(\hat{H} = 0|H = 1) = Q_{\hat{H}}(0),$$

respectively, where

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

and

$$Q_{\hat{H}}(0) = \sum_{u^n, m, v^n} \left[\prod_{i=1}^{n} Q_{UV}(u_i, v_i) \right] f_n(m|u^n)\, g_n(0|m, v^n).$$

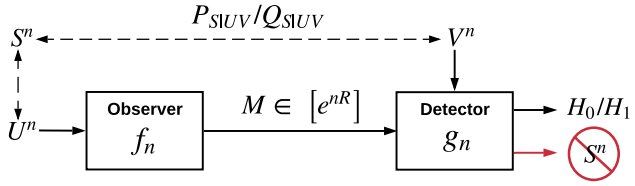


Figure 1. DHT with a privacy constraint.

Let $P_{U^nV^nS^nM\hat{H}}$ and $Q_{U^nV^nS^nM\hat{H}}$ denote the joint distribution of $(U^n, V^n, S^n, M, \hat{H})$ under the null and alternate hypotheses, respectively. For a given type I error probability constraint ϵ, define the minimum type II error probability over all possible detectors as

$$\bar{\beta}_n(f_n, \epsilon) := \inf_{g_n} \beta_n(f_n, g_n), \quad \text{such that } \alpha_n(f_n, g_n) \leq \epsilon. \tag{3}$$

The performance of HT is measured by the error exponent achieved by the test for a given constraint ϵ on the type I error probability, i.e., $\liminf_{n\to\infty} -\frac{1}{n}\log\left(\bar{\beta}_n(f_n,\epsilon)\right)$. Although the goal of the detector is to maximize the error exponent achieved for the HT, it is also curious about the latent r.v. S^n that is correlated with 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 detector. The first is the *equivocation* defined as $H(S^n|M, V^n)$. 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 $d : \mathcal{S} \times \hat{\mathcal{S}} \to [0, D_m]$ with multi-letter distortion defined as

$$d(s^n, \hat{s}^n) := \sum_{i=1}^{n} d(s_i, \hat{s}_i). \tag{4}$$

We will assume the *causal disclosure* assumption, i.e., $\hat{S}_i$ is a function of S^{i-1} in addition to (M, V^n). The goal is to ensure that the error exponent for HT is maximized, while satisfying the constraints on the type I error probability ϵ and the privacy of S^n. In the sequel, we study the trade-off between the rate, error exponent (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 I 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 $f_n : \mathcal{U}^n \to \mathcal{P}(\mathcal{M})$, and $g_n : \mathcal{M} \times \mathcal{V}^n \to \mathcal{P}(\hat{\mathcal{H}})$ such that*

$$\liminf_{n\to\infty} \frac{-\log\left(\bar{\beta}_n(f_n,\epsilon)\right)}{n} \geq \kappa, \tag{5}$$

and for any $\gamma > 0$, there exists an $n_0 \in \mathbb{N}$ such that

$$\inf_{\left\{g_{i,n}^{(r)}\right\}_{i=1}^{n}} \mathbb{E}\left[d\left(S^n, \hat{S}^n\right)|H = j\right] \geq n\Delta_j - \gamma, \ \forall\, n \geq n_0, \ j = 0, 1, \tag{6}$$

where $\hat{S}_i \sim g_{i,n}^{(r)}(\cdot|M, V^n, S^{i-1})$, *and* $g_{i,n}^{(r)} : [e^{nR}] \times \mathcal{V}^n \times \mathcal{S}^{i-1} \to \mathcal{P}(\hat{\mathcal{S}}_i)$ *denotes an arbitrary stochastic reconstruction map at the detector. 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 I error probability constraint* ϵ, *a rate-error exponent-equivocation (It is well known that equivocation as a privacy measure is a special case of average distortion under the causal disclosure assumption and log-loss distortion metric [43]. However, we provide a separate definition of the rate-error exponent-equivocation region for completeness.)* $(R, \kappa, \Lambda_0, \Lambda_1)$ *tuple is* achievable, *if there exists a sequence of encoding and decoding functions* $f_n : \mathcal{U}^n \to \mathcal{P}(\mathcal{M})$ *and* $g_n : [e^{nR}] \times \mathcal{V}^n \to \mathcal{P}(\hat{\mathcal{H}})$ *such that* (5) *is satisfied, and for any* $\gamma > 0$, *there exists a* $n_0 \in \mathbb{N}$ *such that*

$$H(S^n|M, V^n, H = i) \geq n\Lambda_i - \gamma, \ \forall\, n \geq n_0, \ i \in \{0, 1\}. \tag{7}$$

The rate-error exponent-equivocation region $\mathcal{R}_e(\epsilon)$ *is the closure of the set of all such achievable* $(R, \kappa, \Lambda_0, \Lambda_1)$ *tuples for a given* ϵ.

Please note that the privacy measures considered in (6) and (7) are stronger than

$$\liminf_{n\to\infty} \inf_{\left\{g_{i,n}^{(r)}\right\}_{i=1}^{n}} \mathbb{E}\left[\frac{1}{n} d\left(S^n, \hat{S}^n\right) |H = i\right] \geq \Delta_i, \ i = 0, 1, \tag{8}$$

$$\text{and } \liminf_{n\to\infty} \frac{1}{n} H(S^n|M, V^n, H = i) \geq \Lambda_i, \ i = 0, 1, \tag{9}$$

respectively. To see this for the equivocation privacy measure, note that if $H(S^n|M, V^n, H = i) = n\Lambda_i^* - n^a$, $i = 0, 1$, for some $a \in (0, 1)$, then an equivocation pair $(\Lambda_0^*, \Lambda_1^*)$ is achievable under the constraint given in (9), while it is not achievable under the constraint given in (7).

2.3. Relation to Previous Work

Before stating our results, we briefly highlight the differences between our system model and the ones studied in [27,30]. In [27], the observer applies a privacy mechanism to the data before releasing it to the transmitter, which performs further encoding prior to transmission to the detector. More specifically, the observer checks if $U^n \in \mathcal{T}^n_{[P_U]_\delta}$ and if successful, sends the output of a memoryless privacy mechanism applied to U^n, to the transmitter. Otherwise, it outputs a n-length zero-sequence. The privacy mechanism plays the role of randomizing the data (or adding noise) to achieve the desired privacy. Such randomized privacy mechanisms are popular in privacy studies, and have been used in [25,26,61]. In our model, the tasks of coding for privacy and compression are done jointly by using all the available data samples U^n. Also, while we consider the equivocation (and average distortion) between the revealed information and the private part as the privacy measure, in [27], the mutual information between the observer's observations and the output of the memoryless mechanism is the privacy measure. As a result of these differences, there exist some points in the rate-error exponent-privacy trade-off that are achievable in our model, but not in [27]. For instance, a perfect privacy condition $\Lambda_0 = 0$ for testing against independence in ([27], Theorem 2) would imply that the error exponent is also zero, since the output of the memoryless mechanism has to be independent of the observer's observations (under both hypotheses). However, as we later show in Example 2, a positive error exponent is achievable while guaranteeing perfect privacy in our model.

On the other hand, the difference between our model and [30] arises from the difference in the privacy constraint as well as the privacy measure. Specifically, the goal in [30] is to keep U^n private from an

illegitimate eavesdropper, while the objective here is to keep a r.v. S^n that is correlated with U^n private from the detector. Also, we consider the more general average distortion (under causal disclosure) as a privacy measure, in addition to equivocation in [30]. Moreover, as already noted, the equivocation privacy constraint in (7) is more stringent than (9) that is considered in [30]. To satisfy the distortion requirement or the stronger equivocation privacy constraint in (7), we require 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. To achieve this, we use a stochastic encoding scheme to induce the necessary randomness for S^n at the detector, which to the best of our knowledge has not been considered previously in the context of DHT. Consequently, the analysis of the type I and type II error probabilities and privacy achieved are novel. Another subtle yet important difference is that the marginal distributions of U^n and the side information at the eavesdropper are assumed to be the same under the null and alternate hypotheses in [30], which is not the case here. This necessitates separate analysis for the privacy achieved under the two hypotheses.

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

2.4. Supporting Results

Let

$$g_{\mathcal{A}_n}^{(d)}(m, v^n) = \mathbb{1}\left((m, v^n) \in \mathcal{A}_n^c\right) \tag{10}$$

denote a 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 I and type II error probabilities are given by

$$\alpha_n\left(f_n, g_n\right) := P_{MV^n}(\mathcal{A}_n^c) = \mathbb{E}_P\left[\mathbb{1}\left((M, V^n) \in \mathcal{A}_n^c\right)\right], \tag{11}$$

$$\beta_n\left(f_n, g_n\right) := Q_{MV^n}(\mathcal{A}_n) = \mathbb{E}_Q\left[\mathbb{1}\left((M, V^n) \in \mathcal{A}_n\right)\right]. \tag{12}$$

Lemma 1. *Any error exponent that is achievable is also achievable by a deterministic detector of the form given in (10) 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.*

The proof of Lemma 1 is given in Appendix A for completeness. Due to Lemma 1, henceforth we restrict our attention to a deterministic g_n as given in (10).

The next result shows that without loss of generality (w.l.o.g), it is also sufficient to consider $g_{i,n}^{(r)}$ (in Definition 1) to be a deterministic function of the form

$$g_{i,n}^{(r)} = \{\bar{\phi}_{i,n}(\cdot, \cdot, \cdot)\}_{i=1}^n \tag{13}$$

for the minimization in (6), where $\bar{\phi}_{i,n} : \mathcal{M} \times \mathcal{V}^n \times \mathcal{S}^{i-1} \to \hat{\mathcal{S}}$, $i \in [n]$, denotes an arbitrary deterministic function.

Lemma 2. *The infimum in (6) is achieved by a deterministic function $g_{i,n}^{(r)}$ as given in (13), and hence it is sufficient to restrict to such deterministic $g_{i,n}^{(r)}$ in (6).*

The proof of Lemma 2 is given in Appendix B. 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 [60] 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.

Lemma 3. *([60], 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, for $\rho \leq \frac{1}{4}$*

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

The next lemma will be handy in proving Theorems 1 and 2, Proposition 3 and the counter-example for strong converse presented in Section 5.

Lemma 4. *Let (X^n, Y^n) denote n i.i.d. copies of r.v.'s (X, Y), and $P_{X^nY^n} = \prod_{i=1}^n P_{XY}$ and $Q_{X^nY^n} = \prod_{i=1}^n Q_{XY}$ denote two joint probability distributions on (X^n, Y^n). For $\delta > 0$, define*

$$\Pi(x^n, \delta, P_X) := \mathbb{1}\left(x^n \notin \mathcal{T}^n_{[P_X]_\delta}\right). \tag{14}$$

If $P_X \neq Q_X$, then for $\delta > 0$ sufficiently small, there exists $\bar{\delta} > 0$ and $n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|) \in \mathbb{N}$ such that for all $n \geq n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|)$,

$$\|Q_{Y^n}(\cdot) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|1)\| \leq e^{-n\bar{\delta}}. \tag{15}$$

If $P_X = Q_X$, then for any $\delta > 0$, there exists $\bar{\delta} > 0$ and $n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|) \in \mathbb{N}$ such that for all $n \geq n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|)$,

$$\|Q_{Y^n}(\cdot) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|0)\| \leq e^{-n\bar{\delta}}, \tag{16}$$

Also, for any $\delta > 0$, there exists $\bar{\delta} > 0$ and $n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|) \in \mathbb{N}$ such that for all $n \geq n_0(\delta, |\mathcal{X}|, |\mathcal{Y}|)$,

$$\|P_{Y^n}(\cdot) - P_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|0)\| \leq e^{-n\bar{\delta}}. \tag{17}$$

Proof. The proof is presented in Appendix C. □

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

3. 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 1. *For $\epsilon \in (0,1)$, $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e(\epsilon)$ if there exists an auxiliary r.v. W, such that $(V, S) - U - W$, and*

$$R \geq I_P(W; U|V), \tag{18}$$
$$\kappa \leq \kappa^*(P_{W|U}, R), \tag{19}$$
$$\Lambda_0 \leq H_P(S|W, V), \tag{20}$$
$$\Lambda_1 \leq \mathbb{1}\left(P_U = Q_U\right)\ H_Q(S|W, V) + \mathbb{1}\left(P_U \neq Q_U\right)\ H_Q(S|V), \tag{21}$$

where

$$\kappa^*(P_{W|U}, R) := \min\left(E_1(P_{W|U}),\ E_2(R, P_{W|U})\right),$$
$$E_1(P_{W|U}) := \min_{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{L}_1(P_{UW}, P_{VW})} D(P_{\tilde{U}\tilde{V}\tilde{W}}||Q_{UV}P_{W|U}), \tag{22}$$

$$E_2(R, P_{W|U}) := \begin{cases} \min\limits_{P_{\tilde{U}\tilde{V}\tilde{W}} \in \mathcal{L}_2(P_{UW}, P_V)} D(P_{\tilde{U}\tilde{V}\tilde{W}} || Q_{UV} P_{W|U}) + (R - I_P(U; W|V)), & \text{if } I_P(U; W) > R, \\ \infty, & \text{otherwise,} \end{cases} \tag{23}$$

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

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

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

Theorem 2. *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 $\phi : \mathcal{W} \times \mathcal{V} \to \hat{\mathcal{S}}$ and $\phi' : \mathcal{V} \to \hat{\mathcal{S}}$, such that $(V, S) - U - W$ and (18) and (19),*

$$\Delta_0 \leq \min_{\phi(\cdot,\cdot)} \mathbb{E}_P \left[d\left(S, \phi(W, V)\right) \right], \tag{24}$$

$$\text{and } \Delta_1 \leq \mathbb{1}\left(P_U = Q_U\right) \min_{\phi(\cdot,\cdot)} \mathbb{E}_Q \left[d\left(S, \phi(W, V)\right) \right] + \mathbb{1}\left(P_U \neq Q_U\right) \min_{\phi'(\cdot)} \mathbb{E}_Q \left[d\left(S, \phi'(V)\right) \right], \tag{25}$$

are satisfied, where P_{SUVW} and Q_{SUVW} are as defined in Theorem 1.

The proof of Theorems 1 and 2 is given in Apppendix D. While the rate-error exponent trade-off in Theorems 1 and 2 is the same as that achieved by the Shimokawa-Han-Amari (SHA) scheme [7], the coding strategy achieving it is different due to the requirement of the privacy constraint. As mentioned above, in order to obtain a single-letter lower bound for the achievable distortion (and achievable equivocation) 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. For this purpose, we use the so-called likelihood encoder [62,63] (at the observer) in our achievability scheme. The likelihood encoder is a stochastic encoder that induces the necessary randomness for S^n at the detector, and to the best of our knowledge has not been used before in the context of DHT. The analysis of the type I and type II error probabilities and the privacy achieved by our scheme is novel and involves the application of the well-known *channel resolvability* or *soft-covering lemma* [62,64,65]. Properties of the total variation distance between probability distributions mentioned in [43] play a key role in this analysis. The analysis also reveals the interesting fact that the coding schemes in Theorems 1 and 2, although quite different from the SHA scheme, achieves the same lower bound on the error exponent.

Theorems 1 and 2 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 DHT problem without a privacy constraint, in general (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.

4. Optimality Results for Special Cases

4.1. 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

$$H_0 : \ P_{SUYZ} := P_{S|UYZ} P_{U|Z} P_{Y|UZ} P_Z, \tag{26a}$$

and

$$H_1 : \ Q_{SUYZ} := Q_{S|UYZ} P_{U|Z} P_{Y|Z} P_Z, \tag{26b}$$

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 I error probability constraint, i.e.,

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

Assume that the privacy constraint under the alternate hypothesis is inactive. Thus, we are interested in characterizing the set of all tuples $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e$ and $(R, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d$, where

$$\begin{aligned} \Lambda_1 \leq \Lambda_{min} &:= H_Q(S|U, Y, Z), \\ \text{and } \Delta_1 \leq \Delta_{min} &:= \min_{\phi(u,y,z)} \mathbb{E}_Q \left[d\left(S, \phi(U, Y, Z)\right) \right]. \end{aligned} \tag{27}$$

Please note that Λ_{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 observer is more eager to protect S^n when there is a correlation between its own observation and that of the detector, such as the online shopping portal example mentioned in Section 1. In that example, U^n, S^n and Y^n corresponds to shopping behavior, more information about the customer, and customers data available to the shopping portal, respectively.

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

Proposition 1. *For the HT given in* (26), $(R, \kappa, \Lambda_0, \Lambda_{min}) \in \mathcal{R}_e$ *if and only if there exists an auxiliary r.v.* W, *such that* $(Z, Y, S) - U - W$, *and*

$$\kappa \leq I_P(W; Y|Z), \tag{28}$$

$$R \geq I_P(W; U|Z), \tag{29}$$

$$\Lambda_0 \leq H_P(S|W, Z, Y), \tag{30}$$

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

Proof. For TACI, the inner bound in Theorem 1 yields that for $\epsilon \in (0, 1)$, $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e(\epsilon)$ if there exists an auxiliary r.v. W, such that $(Y, Z, S) - U - W$, and

$$R \geq I_P(W; U|Y, Z), \tag{31}$$

$$\kappa \leq \kappa^*(P_{W|U}, R), \tag{32}$$

$$\Lambda_0 \leq H_P(S|W, Y, Z), \tag{33}$$

$$\Lambda_1 \leq H_Q(S|W, Y, Z), \tag{34}$$

where

$$\begin{aligned} &\kappa^*(P_{W|U}, R) := \min \left(E_1(P_{W|U}),\ E_2(R, P_{W|U}) \right), \\ &E_1(P_{W|U}) := \min_{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{L}_1(P_{UW}, P_{YZW})} D(P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} || Q_{UYZ} P_{W|U}), \\ &E_2(R, P_{W|U}) \end{aligned} \tag{35}$$

$$:= \begin{cases} \min\limits_{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{L}_2(P_{UW}, P_{YZ})} D(P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} || Q_{UYZ} P_{W|U}) + (R - I_P(U;W|Y,Z)), & \text{if } I_P(U;W) > R, \\ \infty, & \text{otherwise,} \end{cases} \tag{36}$$

$\mathcal{L}_1(P_{UW}, P_{YZW}) := \{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{P}(\mathcal{U} \times \mathcal{Y} \times \mathcal{Z} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW},\ P_{\tilde{Y}\tilde{Z}\tilde{W}} = P_{YZW}\}$,
$\mathcal{L}_2(P_{UW}, P_{YZ}) := \{P_{\tilde{U}\tilde{Y}\tilde{Z}\tilde{W}} \in \mathcal{P}(\mathcal{U} \times \mathcal{Y} \times \mathcal{Z} \times \mathcal{W}) : P_{\tilde{U}\tilde{W}} = P_{UW},\ P_{\tilde{Y}\tilde{Z}} = P_{YZ},\ H_P(W|Y,Z) \le H(\tilde{W}|\tilde{Y}\tilde{Z})\}$,
$P_{SUYZW} := P_{SUYZ} P_{W|U}$, $Q_{SUYZW} := Q_{S|YZ} P_{U|Z} P_{Y|Z} P_Z P_{W|U}$.

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

$$I_P(W;U) \ge I_P(W;U|Y,Z). \tag{37}$$

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

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

Hence,

$$\kappa^*(P_{W|U}, R) \ge I_P(Y;W|Z). \tag{38}$$

By noting that $\Lambda_{min} \le H_Q(S|W,Y,Z)$ (by the data processing inequality), we have shown that for $\Lambda_1 \le \Lambda_{min}$, $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e$ if (28)–(30) are satisfied. This completes the proof of achievability.

Converse: Let $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e$. 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, S^n, M). Define an auxiliary r.v. $W := (W_T, T)$, where $W_i := (M, Y^{i-1}, S^{i-1}, Z^{i-1}, Z_{i+1}^n)$, $i \in [n]$. Then, we have for sufficiently large n that

$$\begin{aligned} nR &\ge H_P(M) \ge H_P(M|Z^n) \ge I_P(M;U^n|Z^n) \\ &= \textstyle\sum_{i=1}^n I_P(M;U_i|U^{i-1},Z^n) \\ &= \textstyle\sum_{i=1}^n I_P(M,U^{i-1},Z^{i-1},Z_{i+1}^n;U_i|Z_i) && (39) \\ &= \textstyle\sum_{i=1}^n I_P(M,U^{i-1},Z^{i-1},Z_{i+1}^n,Y^{i-1},S^{i-1};U_i|Z_i) && (40) \\ &\ge \textstyle\sum_{i=1}^n I_P(M,Z^{i-1},Z_{i+1}^n,Y^{i-1},S^{i-1};U_i|Z_i) \\ &= \textstyle\sum_{i=1}^n I_P(W_i;U_i|Z_i) = nI_P(W_T;U_T|Z_T,T) \\ &= nI_P(W_T,T;U_T|Z_T) && (41) \\ &= nI_P(W;U|Z). && (42) \end{aligned}$$

Here, (39) follows since the sequences (U^n, Z^n) are memoryless; (40) follows since $(Y^{i-1}, S^{i-1}) - (M, U^{i-1}, Z^n) - U_i$ form a Markov chain; and, (41) follows from the fact that T is independent of all the other r.v.'s.

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

$$\begin{aligned} H(S^n|M,Y^n,Z^n,H=0) &= \textstyle\sum_{i=1}^n H(S_i|M,S^{i-1},Y^n,Z^n,H=0) \\ &\le \textstyle\sum_{i=1}^n H(S_i|M,Y^{i-1},S^{i-1},Z^{i-1},Z_{i+1}^n,Y_i,Z_i,H=0) && (43) \\ &= \textstyle\sum_{i=1}^n H(S_i|W_i,Y_i,Z_i,H=0) \\ &= nH(S_T|W_T,Y_T,Z_T,T,H=0) \end{aligned}$$

$$= nH_P(S|W,Y,Z), \tag{44}$$

where $P_{SUYZW} = P_{SUYZ}P_{W|U}$ for some conditional distribution $P_{W|U}$. In (43), we used the fact that conditioning reduces entropy.

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 $\epsilon_n \to 0$, we have,

$$\begin{aligned} D\left(P_{MY^nZ^n}||Q_{MY^nZ^n}\right) &\geq P_{MY^nZ^n}(\mathcal{A}_n)\log\left(\frac{P_{MY^nZ^n}(\mathcal{A}_n)}{Q_{MY^nZ^n}(\mathcal{A}_n)}\right) + P_{MY^nZ^n}(\mathcal{A}_n^c)\log\left(\frac{P_{MY^nZ^n}(\mathcal{A}_n^c)}{Q_{MY^nZ^n}(\mathcal{A}_n^c)}\right) \qquad (45)\\ &\geq -H(\epsilon_n) - (1-\epsilon_n)\log\left(\bar{\beta}_n\left(f_n,\epsilon_n\right)\right). \end{aligned}$$

Here, (45) follows from the log-sum inequality [60]. Thus,

$$\begin{aligned} \limsup_{n\to\infty}\frac{-\log\left(\bar{\beta}_n\left(f_n,\epsilon_n\right)\right)}{n} &\leq \limsup_{n\to\infty}\frac{1}{n}D\left(P_{MY^nZ^n}||Q_{MY^nZ^n}\right)\\ &= \limsup_{n\to\infty}\frac{1}{n}I_P(M;Y^n|Z^n) \qquad (46)\\ &= H_P(Y|Z) - \liminf_{n\to\infty}\frac{1}{n}H_P(Y^n|M,Z^n), \qquad (47) \end{aligned}$$

where (46) follows since $Q_{MY^nZ^n} = P_{MZ^n}P_{Y^n|Z^n}$. The last term can be single-letterized as follows:

$$\begin{aligned} H_P(Y^n|M,Z^n) &= \textstyle\sum_{i=1}^n H_P(Y_i|Y^{i-1},M,Z^n)\\ &\geq \textstyle\sum_{i=1}^n H_P(Y_i|Y^{i-1},S^{i-1},M,Z^n)\\ &= \textstyle\sum_{i=1}^n H_P(Y_i|Z_i,W_i)\\ &= nH_P(Y_T|Z_T,W_T,T)\\ &= nH_P(Y|Z,W). \qquad (48) \end{aligned}$$

Substituting (48) in (47), we obtain

$$\kappa \leq I_P(Y;W|Z). \tag{49}$$

Also, note that $(Z,Y) - U - W$ holds. To see this, note that (U_i,Y_i,Z_i,S_i) are i.i.d across $i \in [n]$. Hence, any information in W_i on (Y_i,Z_i,S_i) is only through M as a function of U_i, and so given U_i, W_i is independent of (Y_i,Z_i,S_i). The above Markov chain then follows from the fact that T is independent of (U^n,Y^n,Z^n,S^n,M). 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 $\Delta_{min} := \min_{\phi(u,y,z)}\mathbb{E}_Q\left[d\left(S,\phi(U,Y,Z)\right)\right]$.

Proposition 2. *For the HT given in (26), $(R,\kappa,\Delta_0,\Delta_{min}) \in \mathcal{R}_d$ if and only if there exist an auxiliary r.v. W and a deterministic function $\phi : \mathcal{W}\times\mathcal{Y}\times\mathcal{Z} \to \hat{\mathcal{S}}$ such that*

$$R \geq I_P(W;U|Z), \tag{50}$$

$$\kappa \leq I_P(W;Y|Z), \tag{51}$$

$$\Delta_0 \leq \min_{\phi(\cdot,\cdot,\cdot)}\mathbb{E}_P\left[d\left(S,\phi(W,Y,Z)\right)\right], \tag{52}$$

for some P_{SUYZW} as defined in Proposition 1.

Proof. The proof of achievability follows from Theorem 2, similarly to the way Proposition 1 is obtained from Theorem 1. Hence, only differences will be highlighted. Similar to the inequality $\Lambda_{min} \leq H_Q(S|U,Y,Z)$ in the proof of Proposition 1, we need to prove the inequality $\Delta_{min} \leq \mathbb{E}_Q\left[d\left(S,\phi(W,Y,Z)\right)\right]$, where $Q_{SUYZW} := Q_{SUYZ}P_{W|U}$ for some conditional distribution $P_{W|U}$. This can be shown as follows:

$$\begin{aligned}
&\min_{\phi(\cdot,\cdot,\cdot)} \mathbb{E}_Q\left[d\left(S,\phi(W,Y,Z)\right)\right] \\
&= \sum_{u,y,z} Q_{UYZ}(u,y,z) \sum_{w} P_{W|U}(w|u) \min_{\phi(w,y,z)} \sum_{s} Q_{S|UYZ}(s|u,y,z)\, d(s,\phi(w,y,z)) \\
&\geq \sum_{u,y,z} Q_{UYZ}(u,y,z) \sum_{w,s} P_{W|U}(w|u)\, Q_{S|UYZ}(s|u,y,z)\, d(s,\phi^*(u,y,z)) \qquad (53)\\
&\geq \sum_{u,y,z} Q_{UYZ}(u,y,z) \min_{\phi(u,y,z)} \sum_{w,s} P_{W|U}(w|u)\, Q_{S|UYZ}(s|u,y,z)\, d(s,\phi(u,y,z)) \\
&= \sum_{u,y,z} Q_{UYZ}(u,y,z) \min_{\phi(u,y,z)} \sum_{s} Q_{S|UYZ}(s|u,y,z)\, d(s,\phi(u,y,z)) \\
&= \min_{\phi(\cdot,\cdot,\cdot)} \mathbb{E}_Q\left[d\left(S,\phi(U,Y,Z)\right)\right] := \Delta_{min},
\end{aligned}$$

where in (53), $\phi^*(u,y,z)$ 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 Proposition 1. Inequalities (50) and (51) follow similarly as obtained in Proposition 1. We prove (52). Defining $\tilde{\phi}_n(M,Y^n,Z^n,S^{i-1},i) := \bar{\phi}_{i,n}(M,Y^n,Z^n,S^{i-1})$, we have

$$\begin{aligned}
\min_{g_{i,n}^{(r)}} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)\Big|H=0\right] &= \min_{\{\tilde{\phi}_n(m,y^n,z^n,s^{i-1},i)\}_{i=1}^n} \mathbb{E}\left[\sum_{i=1}^n d\left(S_i,\tilde{\phi}_n(M,Y^n,Z^n,S^{i-1},i)\right)\Big|H=0\right] \qquad (54)\\
&= \min_{\{\tilde{\phi}_n(\cdot,\cdot,\cdot,\cdot,\cdot)\}_{i=1}^n} \mathbb{E}\left[\sum_{i=1}^n d\left(S_i,\tilde{\phi}_n(W_i,Z_i,Y_i,Y_{i+1}^n,i)\right)\Big|H=0\right] \\
&\leq \min_{\{\phi(w_i,z_i,y_i,i)\}} \mathbb{E}\left[\sum_{i=1}^n d\left(S_i,\phi(W_i,Z_i,Y_i,i)\right)\Big|H=0\right] \\
&= n \min_{\{\phi(\cdot,\cdot,\cdot,\cdot)\}} \mathbb{E}\left[\mathbb{E}\left[d\left(S_T,\phi(W_T,Z_T,Y_T,T)\right)|T\right]\Big|H=0\right] \\
&= n \min_{\{\phi(\cdot,\cdot,\cdot,\cdot)\}} \mathbb{E}\left[d\left(S_T,\phi(W_T,Z_T,Y_T,T)\right)\Big|H=0\right] \\
&= n \min_{\{\phi(w,z,y)\}} \mathbb{E}\left[d\left(S,\phi(W,Z,Y)\right)\Big|H=0\right],
\end{aligned}$$

where (54) is due to (A1) (in Appendix B). Hence, any Δ_0 satisfying (6) satisfies

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

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

A more general version of Propositions 1 and 2 is claimed in [66] as Theorems 7 and 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 Propositions 1 and 2, we bound the alphabet size of the auxiliary r.v. W in the following lemma, whose proof is given in Appendix E.

Lemma 5. *In Propositions 1 and 2, it suffices to consider auxiliary r.v.'s W such that $|\mathcal{W}| \leq |\mathcal{U}| + 2$.*

The proof of Lemma 5 uses standard arguments based on the Fenchel–Eggleston–Carathéodory's theorem and is given in Appendix E.

Remark 1. *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, $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e$ if and only if there exists an auxiliary r.v. W, such that $(Z, Y, S) - U - W$, and*

$$\kappa \leq I_P(W; Y|Z), \tag{55}$$

$$R \geq I_P(W; U|Z), \tag{56}$$

$$\Lambda_0 \leq H_P(S|W, Z, Y), \tag{57}$$

$$\Lambda_1 \leq H_Q(S|Z, Y), \tag{58}$$

for some P_{SUYZW} as in Proposition 1. 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 $\phi : \mathcal{W} \times \mathcal{Y} \times \mathcal{Z} \to \hat{\mathcal{S}}$ such that (55) and (56),

$$\Delta_0 \leq \min_{\phi(\cdot,\cdot,\cdot)} \mathbb{E}_P \left[d\left(S, \phi(W, Y, Z)\right) \right], \tag{59}$$

$$\Delta_1 \leq \min_{\phi(\cdot,\cdot,\cdot)} \mathbb{E}_Q \left[d\left(S, \phi(Y, Z)\right) \right], \tag{60}$$

are satisfied for some P_{SUYZW} as in Proposition 1.

The computation of the trade-off given in Proposition 1 is challenging despite the cardinality bound on the auxiliary r.v. W provided by Lemma 5, as closed form solutions do not exist in general. To see this, note that the inequality constraints defining $\mathcal{R}_e$ are not convex in general, and hence even computing specific points in the trade-off could be a hard problem. This is evident from the fact that in the absence of the privacy constraint in Proposition 1, i.e., (30), computing the maximum error exponent for a given rate constraint is equivalent to the information bottleneck problem [67], which is known to be a hard non-convex optimization problem. Also, the complexity of brute force search is exponential in $|\mathcal{U}|$, and hence intractable for large values of $|\mathcal{U}|$. Below we provide an example which can be solved in closed form and hence computed easily.

Example 1. *Let $\mathcal{V} = \mathcal{U} = \mathcal{S} = \{0, 1\}$, $V = Y$, $Z =$ constant, $V - S - U$, $P_U(0) = Q_U(0) = 0.5$, $P_{S|U}(0|0) = P_{S|U}(1|1) = Q_{S|U}(0|0) = Q_{S|U}(1|1) = 1 - q$, $P_{V|S}(0|0) = P_{V|S}(1|1) = 1 - p$ and $Q_{V|S}(0|0) = Q_{V|S}(1|1) = 0.5$. Then, $(R, \kappa, \Lambda_0, 0) \in \mathcal{R}_e$ if there exists $r \in [0, 0.5]$ such that*

$$R \geq 1 - h_b(r), \tag{61}$$

$$\kappa \leq 1 - h_b((r * q) * p), \tag{62}$$

$$\Lambda_0 \leq h_b(p) + h_b(q * r) - h_b(p * (q * r)), \tag{63}$$

where for $a, b \in \mathbb{R}$, $a * b := (1-a) \cdot b + (1-b) \cdot a$, *and* $h_b : [0,1] \mapsto [0,1]$ *is the binary entropy function given by*

$$h_b(t) = -(1-t)\log(1-t) - t\log(t).$$

The above characterization (Numerical computation shows that the characterization given in (61)–(63) *is exact even when* $q \in (0,1)$*.) is exact for* $q = 0$*, i.e.,* $(R, \kappa, \Lambda_0, 0) \in \mathcal{R}_e$ *only if there exists* $r \in [0, 0.5]$ *such that* (61)–(63) *are satisfied.*

Proof. Taking $\mathcal{W} = \{0,1\}$, and $P_{W|U}(0|0) = P_{W|U}(1|1) = 1 - r$, the constraints defining the trade-off given in Proposition 1 simplifies to

$$\begin{aligned} I_P(U;W) &= 1 - h_b(r), \\ I_P(V;W) &= 1 - h_b((r * q) * p), \\ H_P(S|V,W) &= H_P(S|W) - I_P(S;V|W) \\ &= H_P(S|W) + H_P(V|S) - H_P(V|W) \\ &= h_b(r * q) + h_b(p) - h_b(p * (q * r)). \end{aligned}$$

On the other hand, if $q = 0$, note that $S = U$. Hence, the same constraints can be bounded as follows:

$$\begin{aligned} I_P(U;W) &= 1 - H_P(U|W), \\ I_P(V;W) &= 1 - H_P(V|W) \leq 1 - h_b\left(h_b^{-1}(H(U|W)) * p\right), \qquad (64) \\ H_P(U|V,W) &= H_P(U|W) + H_P(V|U) - H_P(V|W) \\ &\leq h_b(p) + H_P(U|W) - h_b\left(h_b^{-1}(H_P(U|W)) * p\right), \qquad (65) \end{aligned}$$

where $h_b^{-1} : [0,1] \mapsto [0, 0.5]$ is the inverse of the binary entropy function. Here, the inequality in (64) and (65) follows by an application of Mrs Gerber's lemma [68], since $V = U \oplus N_p$ under the null hypothesis and $N_p \sim Ber(p)$ is independent of U and W. Also, $\Lambda_{min} = 0$ since $S = U$. Noting that $H_P(U|W) \in [0,1]$, and defining $r := h_b^{-1}(H_P(U|W)) \in [0, 0.5]$, the result follows. □

Figure 2 depicts the curve $(1 - h_b(r), 1 - h_b(p * (q * r)), h_b(p) + h_b(r * q) - h_b(p * (r * q)))$ for $q = 0$ and $p \in \{0.15, 0.25, 0.35\}$, as r is varied in the range $[0, 0.5]$. The projection of this curve on the $R - \kappa$ and $\kappa - \Lambda_0$ plane is shown in Figures 3a,b, respectively, for $q \in \{0, 0.1\}$ and the same values of p. As expected, the error exponent κ increases with rate R while the equivocation Λ_0 decreases with κ at the boundary of $\mathcal{R}_e$.

Proposition 1 (resp. Proposition 2) provide a characterization of $\mathcal{R}_e$ (resp. $\mathcal{R}_d$) under the condition of vanishing type I 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 I error probability constraint $\epsilon \in (0,1)$, and hence known as a *strong converse* result.

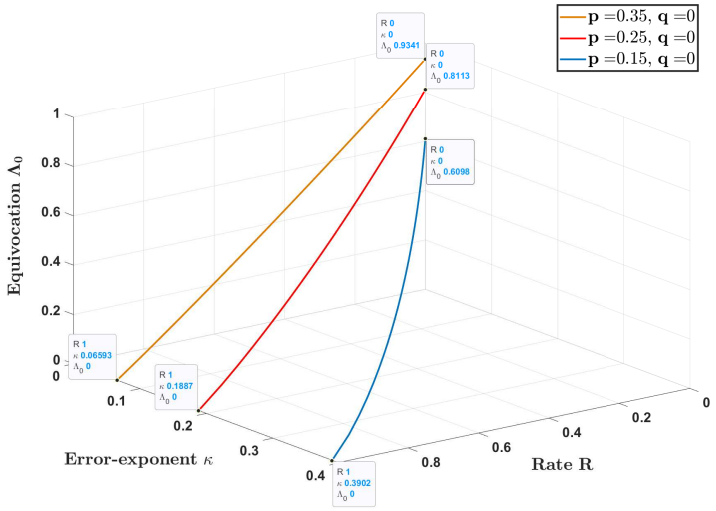
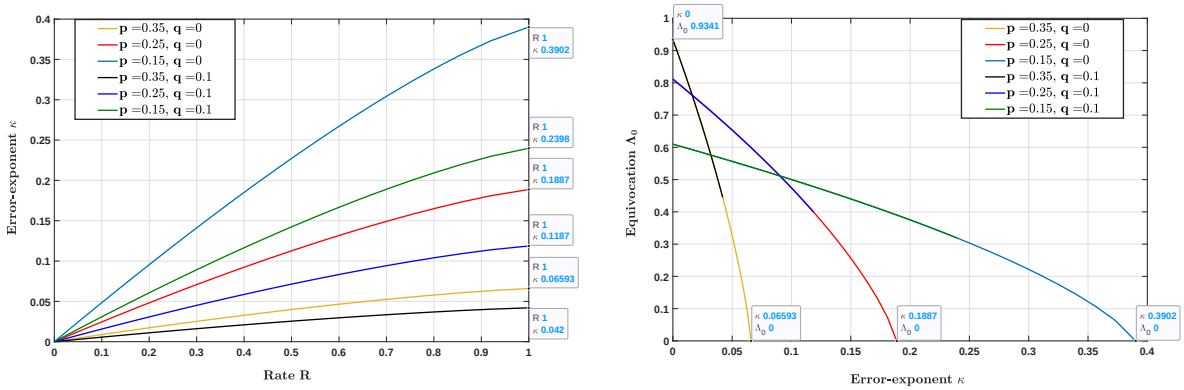


Figure 2. (R, κ, Λ_0) trade-off at the boundary of $\mathcal{R}_e$ in Example 1 (Axes units are in bits).



(**a**) $R - \kappa$ trade-off (Axes units are in bits) (**b**) $\kappa - \Lambda_0$ trade-off (Axes units are in bits)

Figure 3. Projections of Figure 2 in the $R - \kappa$ plane and $\kappa - \Lambda_0$ plane.

4.2. Zero-Rate Compression

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

$$\lim_{n\to\infty} \frac{\log(|\mathcal{M}|)}{n} = 0. \tag{66}$$

Please note that (66) 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. Propositions 3 and 4 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. Lemma 4 serves as a crucial tool for this purpose. We next state the results. Let

$$\Delta_0^{max} := \min_{\phi'(\cdot)} \mathbb{E}_P \left[d\left(S, \phi'(V)\right) \right], \tag{67a}$$

$$\text{and } \Delta_1^{max} := \min_{\phi'(\cdot)} \mathbb{E}_Q \left[d\left(S, \phi'(V)\right) \right]. \tag{67b}$$

Proposition 3. *For $\epsilon \in (0,1)$, $(0, \kappa, \Delta_0, \Delta_1) \in \mathcal{R}_d(\epsilon)$ if and only if it satisfies,*

$$\kappa \leq \min_{P_{\tilde{U}\tilde{V}} \in \mathcal{L}'(P_U, P_V)} D(P_{\tilde{U}\tilde{V}} || Q_{UV}), \tag{68}$$

$$\Delta_0 \leq \Delta_0^{max}, \tag{69}$$

$$\Delta_1 \leq \Delta_1^{max}, \tag{70}$$

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

$$\mathcal{L}'(P_U, P_V) = \{P_{\tilde{U}\tilde{V}} \in \mathcal{P}(\mathcal{U} \times \mathcal{V}) : P_{\tilde{U}} = P_U,\ P_{\tilde{V}} = P_V\}.$$

Proof. First, we prove that $(0, \kappa, \Delta_0, \Delta_1)$ satisfying (68)–(70) 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 observer sends the message $M = 1$ if $U^n \in \mathcal{T}^n_{[P_U]_\delta}$, $\delta > 0$, and $M = 0$ otherwise.
Decoding: The detector declares $\hat{H} = 0$ if $M = 1$ and $V^n \in \mathcal{T}^n_{[P_V]_\delta}$, $\delta > 0$. Otherwise, $\hat{H} = 1$ is declared.

We analyze the type I and type II error probabilities for the above scheme. Please note that for any $\delta > 0$, the weak law of large numbers implies that

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

Hence, the type I error probability tends to zero, asymptotically. The type II error probability can be written as follows:

$$\begin{aligned}\beta_n(f_n, g_n) &= \mathbb{P}(U^n \in \mathcal{T}^n_{[P_U]_\delta} \cap V^n \in \mathcal{T}^n_{[P_V]_\delta}) | H = 1) \\ &= \sum_{\substack{u^n \in \mathcal{T}^n_{[P_U]_\delta}, \\ v^n \in \mathcal{T}_{[P_V]_\delta}}} Q_{U^nV^n}(u^n, v^n) \leq (n+1)^{|\mathcal{U}||\mathcal{V}|} e^{-n(\kappa^* - O(\delta))} = e^{-n\left(\kappa^* - \frac{|\mathcal{U}||\mathcal{V}| \log(n+1)}{n} - O(\delta)\right)},\end{aligned}$$

where

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

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

$$\Pi(U^n, \delta, P_U) := \mathbb{1}\left(U^n \notin \mathcal{T}^n_{[P_U]_\delta}\right), \tag{71}$$

$$\rho_n^{(0)}(\delta) := \left\| P_{S^nV^n}(\cdot) - P_{S^nV^n|\Pi(U^n, \delta, P_U)}(\cdot|0) \right\|,, \tag{72}$$

$$\rho_n^{(1)}(\delta) := \left\| Q_{S^nV^n}(\cdot) - Q_{S^nV^n|\Pi(U^n, \delta, P_U)}(\cdot|1) \right\|, \tag{73}$$

$$\phi_n'(v^n) := (\phi'(v_1), \cdots, \phi'(v_n)),$$

we can write

$$\left| \min_{\{\bar{\phi}_i(m, v^n, s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n, \hat{S}^n\right) | H = 0\right] - n \min_{\phi'(v)} \mathbb{E}_P\left[d\left(S, \phi'(V)\right)\right] \right|$$

$$
\begin{aligned}
&= \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right] - \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|H=0\right] \Big| \\
&\le \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right] - \mathbb{P}\left(M=1|H=0\right) \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=0\right] \Big| \\
&\quad + \mathbb{P}\left(M=0|H=0\right) \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=0\right] \\
&\le \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right] - \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=0\right] \Big| \\
&\quad + \mathbb{P}\left(M=0|H=0\right) \Big[\min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=0\right] \\
&\qquad + \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=0\right] \Big] \\
&= \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right] - \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|\Pi(U^n,\delta,P_U)=0,H=0\right] \Big| \\
&+ \mathbb{P}\left(\Pi(U^n,\delta,P_U)=1|H=0\right) \Big[\min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=0\right] \\
&\qquad\qquad + \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=0\right] \Big] \qquad (74) \\
&\le nD_m\rho_n^{(0)}(\delta) + 2\,e^{-n\Omega(\delta)}nD_m \qquad (75) \\
&\xrightarrow{(n)} 0, \qquad (76)
\end{aligned}
$$

where (74) is since $\Pi(U^n,\delta,P_U) = 1-M$ with probability one by the encoding scheme; (75) follows from

$$\mathbb{P}\left(\Pi(U^n,\delta,P_U)=1|H=0\right) = \mathbb{P}\left(U^n \notin \mathcal{T}^n_{[P_U]_\delta}|H=0\right) \le e^{-n\Omega(\delta)} \qquad (77)$$

and ([43], Property 2(b)); and, (76) is due to (17). Similarly, it can be shown using (16) that if $Q_U = P_U$, then

$$\Big| \min_{\{\bar{\phi}_{i,n}(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right] - n\min_{\phi'(v)} \mathbb{E}_Q\left[d\left(S,\phi'(V)\right)\right] \Big| \xrightarrow{(n)} 0. \qquad (78)$$

On the other hand, if $Q_U \neq P_U$ and δ is small enough, we have

$$\mathbb{P}\left(M=0|H=1\right) = \mathbb{P}\left(\Pi(U^n,\delta,P_U)=1|H=1\right) \ge 1 - e^{-n(D(P_U||Q_U)-O(\delta))} \xrightarrow{(n)} 1. \qquad (79)$$

Hence, we can write for δ small enough,

$$
\begin{aligned}
&\Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right] - n\min_{\phi'(v)} \mathbb{E}_Q\left[d\left(S,\phi'(V)\right)\right] \Big| \\
&= \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right] - \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|H=1\right] \Big| \\
&\le \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right] - \mathbb{P}\left(M=0|H=0\right) \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=1\right] \Big| \\
&\quad + \mathbb{P}\left(M=1|H=1\right) \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=1\right] \\
&\le \Big| \min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right] - \min_{\phi'_n(v^n)} \mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=1\right] \Big|
\end{aligned}
$$

$$
\begin{aligned}
&+\mathbb{P}\left(M=1|H=1\right)\Big[\min_{\phi'_n(v^n)}\mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=1\right]\\
&\qquad\qquad+\min_{\phi'_n(v^n)}\mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=1\right]\Big]\\
&=\Big|\min_{\{\bar{\phi}_i(m,v^n,s^{i-1})\}_{i=1}^n}\mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right]-\min_{\phi'_n(v^n)}\mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|\Pi(U^n,\delta,P_U)=1,H=1\right]\Big|\\
&+\mathbb{P}\left(\Pi(U^n,\delta,P_U)=0|H=1\right)\Big[\min_{\phi'_n(v^n)}\mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=1,H=1\right]\\
&\qquad\qquad+\min_{\phi'_n(v^n)}\mathbb{E}\left[d\left(S^n,\phi'_n(V^n)\right)|M=0,H=1\right]\Big] \qquad (80)\\
&\leq nD_m\rho_n^{(1)}(\delta)+2\,e^{-n(D(P_U||Q_U)-O(\delta))}nD_m \qquad (81)\\
&\xrightarrow{(n)}0, \qquad (82)
\end{aligned}
$$

where (80) is since $\Pi(U^n,\delta,P_U)=1-M$ with probability one; (81) is due to (79) and ([43], Property 2(b)); and, (82) follows from (15). This completes the proof of the achievability.

We next prove the converse. Please note that by the strong converse result in [8], the right hand side (R.H.S) of (68) is an upper bound on the achievable error exponent for all $\epsilon\in(0,1)$ even without a privacy constraint (hence, also with a privacy constraint). Also,

$$
\begin{aligned}
\min_{g_{i,n}^{(r)}}\mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right]&\leq\min_{\{\phi'(v_i)\}_{i=1}^n}\sum_{i=1}^n\mathbb{E}_{P_{S_iV_i}}\left[d\left(S_i,\phi'(V_i)\right)\right] \qquad (83)\\
&=n\min_{\{\phi'(v)\}}\mathbb{E}_P\left[d(S,\phi'(V))\right].
\end{aligned}
$$

Here, (83) follows from the fact that the detector can always reconstruct $\hat{S}_i$ as a function of V_i for $i\in[n]$. Similarly,

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

Hence, any achievable Λ_0 and Λ_1 must satisfy (69) and (70), respectively. This completes the proof. □

The following Proposition is the analogous result to Proposition 3 when the privacy measure is equivocation.

Proposition 4. *For $\epsilon\in(0,1)$, $(0,\kappa,\Lambda_0,\Lambda_1)\in\mathcal{R}_e(\epsilon)$ if and only if it satisfies (68) and*

$$
\begin{aligned}
\Lambda_0&\leq H_P(S|V), \qquad (84)\\
\Lambda_1&\leq H_Q(S|V). \qquad (85)
\end{aligned}
$$

Proof. For proving the achievability part, the encoding and decoding scheme is the same as in Proposition 3. Hence, the analysis of the error exponent given in Proposition 3 holds. To lower bound the equivocation of S^n at the detector, defining $\Pi(U^n,\delta,P_U)$, $\rho_n^{(0)}(\delta)$ and $\rho_n^{(1)}(\delta)$ as in (71)–(73), we can write

$$
\begin{aligned}
&\left|nH_P(S|V)-H(S^n|M,V^n,H=0)\right|\\
&=\left|H(S^n|V^n,H=0)-H(S^n|M,V^n,H=0)\right|\\
&\leq\left|H(S^n,V^n|H=0)-H(S^n,V^n|M,H=0)\right|
\end{aligned}
$$

$$
\begin{aligned}
&\leq \left|H(S^n,V^n|H=0) - \mathbb{P}\left(M=1|H=0\right)\ H(S^n,V^n|M=1,H=0)\right| \\
&\qquad + \mathbb{P}\left(M=0|H=0\right) H(S^n,V^n|M=0,H=0) \\
&\leq \left|H(S^n,V^n|H=0) - H(S^n,V^n|M=1,H=0)\right| \\
&\qquad + \mathbb{P}\left(M=0|H=0\right)\left(H(S^n,V^n|M=1,H=0) + H(S^n,V^n|M=0,H=0)\right) \\
&\leq \left|H(S^n,V^n|H=0) - H(S^n,V^n|\Pi(U^n,\delta,P_U)=0,H=0)\right| \\
&\qquad + \mathbb{P}\left(\Pi(U^n,\delta,P_U)=1|H=0\right)\left(H(S^n,V^n|M=1,H=0) + H(S^n,V^n|M=0,H=0)\right) \\
&\overset{(n)}{\leq} -2\rho_n^{(0)}(\delta)\log\left(\frac{\rho_n^{(0)}(\delta)}{|\mathcal{S}|^n|\mathcal{V}|^n}\right) + 2\,e^{-n\Omega(\delta)}\log\left(|\mathcal{S}|^n|\mathcal{V}|^n\right) \qquad (86) \\
&\xrightarrow{(n)} 0, \qquad (87)
\end{aligned}
$$

where (86) follows due to Lemma 3, ([60], Lemma 2.12) and the fact that entropy of a r.v. is bounded by the logarithm of cardinality of its support; and, (87) follows from (17) in Lemma 4 since $\delta > 0$. In a similar way, it can be shown using (16) that if $Q_U = P_U$, then

$$
\left|H(S^n|V^n,H=1) - H(S^n|M,V^n,H=1)\right| \xrightarrow{(n)} 0. \qquad (88)
$$

On the other hand, if $Q_U \neq P_U$ and δ is small enough, we can write

$$
\begin{aligned}
&|nH_Q(S|V) - H(S^n|M,V^n,H=1)| \\
&= |H(S^n|V^n,H=1) - H(S^n|M,V^n,H=1)| \\
&\leq |H(S^n,V^n|H=1) - H(S^n,V^n|M,H=1)| \\
&\leq |H(S^n,V^n|H=1) - H(S^n,V^n|M=0,H=1)| \\
&\quad + \mathbb{P}\big(\Pi(U^n,\delta,P_U)=0|H=1\big)\left(H(S^n,V^n|M=0,H=1) + H(S^n,V^n|M=1,H=1)\right) \\
&\leq -2\rho_n^{(1)}(\delta)\log\left(\frac{\rho_n^{(1)}(\delta)}{|\mathcal{S}|^n|\mathcal{V}|^n}\right) + 2\,e^{-n(D(P_U||Q_U)-O(\delta))}\log\left(|\mathcal{S}|^n|\mathcal{V}|^n\right), \qquad (89)
\end{aligned}
$$

where (89) follows from Lemma 3 and (79). It follows from (15) in Lemma 4 that for $\delta > 0$ sufficiently small, $\rho_n^{(1)}(\delta) \leq e^{-n\bar{\delta}}$ for some $\bar{\delta} > 0$, thus implying that the R.H.S. of (89) tends to zero. This completes the proof of achievability.

The converse follows from the results in [6,8] that the R.H.S of (68) is the optimal error exponent achievable for all values of $\epsilon \in (0,1)$ even when there is no privacy constraint, and the following inequality

$$
H(S^n|M,V^n,H=j) \leq H(S^n|V^n,H=j),\ j=0,1. \qquad (90)
$$

This concludes the proof of the Proposition. □

In Section 2.2, we mentioned that it is possible to achieve a positive error exponent 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 $Z =$ 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 2. *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* (31)–(34), *and,* (37) *and* (38) *that* $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e(\epsilon)$, $\epsilon \in (0,1)$ *if*

$$\begin{aligned} R &\geq I_P(W;U), \\ \kappa &\leq I_P(W;Y), \\ \Lambda_0 &\leq H_P(S|W,Y), \\ \Lambda_1 &\leq H_Q(S|W,Y) = H_Q(S|W), \end{aligned}$$

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 error exponent while ensuring maximum privacy under both the null and alternate hypothesis, i.e., the tuple* $(1,1,2,2) \in \mathcal{R}_e(\epsilon)$, $\forall\, \epsilon \in (0,1)$.

5. A Counter-Example to the Strong Converse

Ahlswede and Csiszár obtained a strong converse result for the DHT problem without a privacy constraint in [5], where they showed that for any positive rate R, the optimal achievable error exponent is independent of the type I 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 counter-example that this is not the case in general. The basic idea used in the counter-example is a "time-sharing" argument which is used to construct from a given coding scheme that achieves the optimal rate-error exponent-equivocation trade-off under a vanishing type I error probability constraint, a new coding scheme that satisfies the given type I error probability constraint ϵ^* and the same error exponent as before, yet achieves a higher equivocation for S^n at the detector. This concept has been used previously in other contexts, e.g., in the characterization of the first-order maximal channel coding rate of additive white gaussian noise (AWGN) channel in the finite block-length regime [69], and subsequently in the characterization of the second order maximal coding rate in the same setting [70]. However, we will provide a self-contained proof of the counter-example by using Lemma 4 for this purpose.

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 $(R, \kappa, \Lambda_0, \Lambda_1) \in \mathcal{R}_e(\epsilon)$ 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 $\Lambda_1 \leq \Lambda_{min}$. Then, from the optimal single-letter characterization of $\mathcal{R}_e$ given in Proposition 1, it follows by taking $W = U$ that $(H_P(U), I_P(V;U), H_P(S|V,U), \Lambda_{min}) \in \mathcal{R}_e$. Please note that $I_P(V;U)$ is the maximum error exponent achievable for any type I error probability constraint $\epsilon \in (0,1)$, even when U^n is observed directly at the detector. Thus, for vanishing type I error probability constraint $\epsilon \to 0$ 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 Proposition 1, the coding scheme achieving this tuple is as follows:

1. Quantize u^n to codewords in $\mathcal{B}_n = \{u^n(j) \in \mathcal{T}^n_{[P_U]_\delta},\ j \in [e^{n(H_P(U)+\eta)}]\}$ and send the index of quantization to the detector, i.e., if $u^n \in \mathcal{T}^n_{[P_U]_\delta}$, send $M = j$, where j is the index of u^n in $\mathcal{B}_n$. Else, send $M = 0$.
2. At the detector, if $M = 0$, declare $\hat{H} = 1$. Else, declare $\hat{H} = 0$ if $(u^n(M), v^n) \in \mathcal{T}^n_{[P_{UV}]_{\delta'}}$ for some $\delta' > \delta$, and $\hat{H} = 1$ otherwise.

The type I 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 $u^n \in \mathcal{T}^n_{[P_U]_\delta}$, send $M = j$ with probability $1 - \epsilon^*$, where j is the index of u^n in $\mathcal{B}_n$, and with probability ϵ^*, send $M = 0$. If $u^n \notin \mathcal{T}^n_{[P_U]_\delta}$, send $M = 0$.
2. At the detector, if $M = 0$, declare $\hat{H} = 1$. Else, declare $\hat{H} = 0$ if $u^n(M), v^n) \in \mathcal{T}^n_{[P_{UV}]_{\delta'}}$ for some $\delta' > \delta$, and $\hat{H} = 1$ otherwise.

It is easy to see that for this modified coding scheme, the type I error probability is asymptotically equal to ϵ^*, while the error exponent remains the same as $I(V;U)$ since the probability of declaring $\hat{H} = 0$ is decreased. Recalling that $\Pi(u^n, \delta, P_U) := \mathbb{1}\left(u^n \notin \mathcal{T}^n_{[P_U]_\delta}\right)$, we also have

$$
\begin{aligned}
&\frac{1}{n}H\big(S^n|M,V^n,H=0\big)\\
&=(1-\gamma_n)(1-\epsilon^*)\frac{1}{n}H\big(S^n|U^n,V^n,\Pi(U^n,\delta,P_U)=0,H=0\big)+(1-\gamma_n)\,\epsilon^*\\
&\quad\frac{1}{n}H\big(S^n|M=0,V^n,\Pi(U^n,\delta,P_U)=0,H=0\big)+\gamma_n\,\frac{1}{n}H\big(S^n|M=0,V^n,\Pi(U^n,\delta,P_U)=1,H=0\big)\\
&\geq(1-\gamma_n)(1-\epsilon^*)\,\left(H_P\left(S|U,V\right)-\gamma_n''\right)+(1-\gamma_n)\,\epsilon^*\,\frac{1}{n}H\big(S^n|M=0,V^n,\Pi(U^n,\delta,P_U)=0,H=0\big)\\
&\quad+\gamma_n\,\frac{1}{n}H\big(S^n|M=0,V^n,\Pi(U^n,\delta,P_U)=1,H=0\big) \qquad (91)\\
&>(1-\gamma_n)(1-\epsilon^*)\,\left(H_P\left(S|U,V\right)-\gamma_n''\right)+(1-\gamma_n)\,\epsilon^*\,\left(H_P(S|U,V)-\frac{\gamma_n'}{n}\right)\\
&\quad+\gamma_n\,\frac{1}{n}H\big(S^n|M=0,V^n,H=0,\Pi(U^n,\delta,P_U)=1\big) \qquad (92)\\
&=(1-\gamma_n)(1-\epsilon^*)\,\left(H_P\left(S|U,V\right)-\gamma_n''\right)+(1-\gamma_n)\,\epsilon^*\left(H_P\left(S|U,V\right)-\frac{\gamma_n'}{n}\right)+\gamma_n''' \qquad (93)\\
&=(1-\gamma_n)H_P\left(S|U,V\right)-\bar{\gamma}_n, \qquad (94)
\end{aligned}
$$

where $\{\gamma_n''\}_{n\in\mathbb{N}}$ denotes some sequence of positive numbers such that $\gamma_n'' \xrightarrow{(n)} 0$, and

$$
\begin{aligned}
&\gamma_n := \mathbb{P}\left(U^n \notin \mathcal{T}^n_{[P_U]_\delta}\big|H=0\right) \leq e^{-n\Omega(\delta)} \xrightarrow{(n)} 0, \qquad (95)\\
&\gamma_n' := -2\rho_n^*\log\left(\frac{2\rho_n^*}{|\mathcal{S}|^n}\right),\\
&\rho_n^* := \left\|P_{S^nV^n|\Pi(U^n,\delta,P_U),M}(\cdot|0,0)-P_{S^nV^n}(\cdot)\right\| = \left\|P_{S^nV^n|\Pi(U^n,\delta,P_U)}(\cdot|0)-P_{S^nV^n}(\cdot)\right\|, \qquad (96)\\
&\gamma_n''' := \frac{\gamma_n}{n}H(S^n|M=0,V^n,,H=0,\Pi(U^n,\delta,P_U)=1) \xrightarrow{(n)} 0, \qquad (97)
\end{aligned}
$$

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

Equation (91) follows similarly to the proof of Theorem 1 in [71]. Equation (92) is obtained as follows:

$$\begin{aligned}
&\frac{1}{n}H\left(S^n|M=0,V^n,I_U(U^n,\delta)=0,H=0\right)\\
&\geq \frac{1}{n}H\left(S^n|V^n,H=0\right)-\frac{\gamma_n'}{n} &(98)\\
&> H_P(S|U,V)-\frac{\gamma_n'}{n}. &(99)
\end{aligned}$$

Here, (98) is obtained by an application of Lemma 3; and (99) is due to the assumption that $H_P(S|U,V) < H_P(S|V)$.

It follows from Lemma 4 that $\rho_n^* \xrightarrow{(n)} 0$, which in turn implies that

$$\frac{\gamma_n'}{n} \xrightarrow{(n)} 0. \tag{100}$$

From (95), (97) and (100), we have that $\bar{\gamma}_n \xrightarrow{(n)} 0$. Hence, equation (94) implies that $(H_P(U), I_P(V;U), \Lambda_0^*, \Lambda_{min}) \in \mathcal{R}_e(\epsilon^*)$ for some $\Lambda_0^* > H_P(S|U,V)$. Since $(H_P(U), I_P(V;U), \Lambda_0^*, \Lambda_{min}) \notin \mathcal{R}_e$, this implies that in general, the strong converse does not hold for HT with an equivocation privacy constraint. The same counter-example 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.

6. Conclusions

We have studied the DHT problem with a privacy constraint, with equivocation and average distortion under a causal disclosure assumption 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 DHT does not hold when there is an additional privacy constraint in the system. 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. Yet another important topic worth exploring is the trade-off between rate, error probability and privacy in the finite sample regime for the setting considered in this paper.

Author Contributions: Conceptualization, S.S., A.C. and D.G.; writing—original draft preparation, S.S.; supervision, A.C. and D.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the European Research Council Starting Grant project BEACON (grant agreement number 677854).

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

HT	Hypothesis testing
DHT	Distributed hypothesis testing
TACI	Testing against conditional independence

TAI	Testing against independence
DP	Differential privacy
KL	Kullback–Leibler
SHA	Shimokawa-Han-Amari

Appendix A. Proof of Lemma 1

Please note that for a stochastic detector, the type I and type II error probabilities are linear functions of $P_{\hat{H}|M,V^n}$. As a result, for each fixed n and f_n, $\alpha_n(f_n, g_n)$ and $\beta_n(f_n, g_n)$ for a stochastic detector g_n can be thought of as the type I and type II errors achieved by "time-sharing" among a finite number of deterministic detectors. To see this, consider some ordering on the elements of the set $\mathcal{M} \times \mathcal{V}^n$ and let $\nu_i := P_{\hat{H}|M,V^n}(0|i)$, $i \in [1 : N]$, where i denotes the i^{th} element of $\mathcal{M} \times \mathcal{V}^n$ and $N = |\mathcal{M} \times \mathcal{V}^n|$. Then, we can write

$$P_{\hat{H}|M,V^n} = \begin{bmatrix} \nu_1 & 1-\nu_1 \\ \nu_2 & 1-\nu_2 \\ \vdots & \vdots \\ \nu_N & 1-\nu_N \end{bmatrix}.$$

Then, it is easy to see that $P_{\hat{H}|M,V^n} = \sum_{i=1}^{N} \nu_i I_i$, where $I_i := [e_i \; 1-e_i]$ and e_i is an N length vector with 1 at the i^{th} component and 0 elsewhere. Now, suppose $(\alpha_n^{(1)}, \beta_n^{(1)})$ and $(\alpha_n^{(2)}, \beta_n^{(2)})$ denote the pair of type I and type II error probabilities achieved by deterministic detectors $g_n^{(1)}$ and $g_n^{(2)}$, respectively. Let $\mathcal{A}_{1,n}$ and $\mathcal{A}_{2,n}$ denote their corresponding acceptance regions for H_0. Let $g_n^{(\theta)}$ denote the stochastic detector formed by using $g_n^{(1)}$ and $g_n^{(2)}$ with probabilities θ and $1-\theta$, respectively. From the above-mentioned linearity property, it follows that $g_n^{(\theta)}$ achieves type I and type II error probabilities of $\alpha_n\left(f_n, g_n^{(\theta)}\right) = \theta\alpha_n^{(1)} + (1-\theta)\alpha_n^{(2)}$ and $\beta_n\left(f_n, g_n^{(\theta)}\right) = \theta\beta_n^{(1)} + (1-\theta)\beta_n^{(2)}$, respectively. Let $r(\theta) = \min(\theta, 1-\theta)$. Then, for $\theta \in (0,1)$,

$$-\frac{1}{n}\log\left(\beta_n\left(f_n, g_n^{(\theta)}\right)\right) \leq \min\left(-\frac{1}{n}\log\beta_n^{(1)}, -\frac{1}{n}\log\beta_n^{(2)}\right) - \frac{1}{n}\log(r(\theta)).$$

Hence, either

$$\alpha_n^{(1)} \leq \alpha_n\left(f_n, g_n^{(\theta)}\right) \text{ and } -\frac{1}{n}\log\beta_n^{(1)} \geq -\frac{1}{n}\log\left(\beta_n\left(f_n, g_n^{(\theta)}\right)\right) + \frac{1}{n}\log(r(\theta)),$$

or

$$\alpha_n^{(2)} \leq \alpha_n\left(f_n, g_n^{(\theta)}\right) \text{ and } -\frac{1}{n}\log\beta_n^{(2)} \geq -\frac{1}{n}\log\left(\beta_n\left(f_n, g_n^{(\theta)}\right)\right) + \frac{1}{n}\log(r(\theta)).$$

Thus, since $\frac{1}{n}\log(r(\theta)) \xrightarrow{(n)} 0$, a stochastic detector does not offer any advantage over deterministic detectors in the trade-off between the error exponent and the type I error probability.

Appendix B. Proof of Lemma 2

Let $\tilde{P}^{(\mathcal{C}_n,0)}_{S^nU^nV^nM\hat{S}^n} = P_{S^nU^nV^nM} \prod_{i=1}^{n} \tilde{P}_{\hat{S}_i|M,V^n,S^{i-1}}$ and $\tilde{P}^{(\mathcal{C}_n,1)}_{S^nU^nV^nM\hat{S}^n} = Q_{S^nU^nV^nM} \prod_{i=1}^{n} \tilde{P}_{\hat{S}_i|M,V^n,S^{i-1}}$ denote the joint distribution of the r.v.'s $(S^n, U^n, V^n, M, \hat{S}^n)$ under hypothesis H_0 and H_1, respectively, where $\tilde{P}_{\hat{S}_i|M,V^n,S^{i-1}}$ denotes $g_{i,n}^{(r)}$ for $i \in [n]$. Then, we have

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

where

$$
\phi_{ij}(m,v^n,s^{i-1}) = \arg\min_{\hat{s}\in\hat{\mathcal{S}}} \mathbb{E}_{\tilde{P}^{(j)}_{S_i|M,V^n,S^{i-1}}(\cdot|m,v^n,s^{i-1})}\left[d(S_i,\hat{s})\right].
$$

Continuing, we have

$$
\begin{aligned}
&\min_{g_{i,n}^{(r)}} \mathbb{E}\left[d\left(S^n, \hat{S}^n\right)|H=j\right] \\
&= \frac{1}{n}\sum_{i=1}^n \sum_{m,v^n,s^{i-1}} \tilde{P}^{(j)}_{MV^nS^{i-1}}(m,v^n,s^{i-1}) \min_{\phi_i(m,v^n,s^{i-1})} \mathbb{E}_{\tilde{P}^{(j)}_{S_i|M,V^n,S^{i-1}}(\cdot|m,v^n,s^{i-1})}\left[d\left(S_i, \phi_i(m,v^n,s^{i-1})\right)\right] \\
&= \min_{\{\phi_i(m,v^n,s^{i-1})\}_{i=1}^n} \frac{1}{n}\sum_{i=1}^n \mathbb{E}_{\tilde{P}^{(j)}}\left[d\left(S_i, \phi_i(M,V^n,S^{i-1})\right)\right]. \qquad \text{(A1)}
\end{aligned}
$$

This completes the proof.

Appendix C. Proof of Lemma 4

We will first prove (15). Fix $\delta > 0$. For $\gamma > 0$, define the following sets:

$$
\begin{aligned}
\mathcal{B}^{\delta}_{0,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[P_Y]_\gamma} : P_{Y^n}(y^n) \geq P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right\}, \qquad \text{(A2)} \\
\mathcal{C}^{\delta}_{0,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[P_Y]_\gamma} : P_{Y^n}(y^n) < P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right\}, \qquad \text{(A3)} \\
\mathcal{B}^{\delta}_{1,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[Q_Y]_\gamma} : Q_{Y^n}(y^n) \geq Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right\}, \\
\mathcal{C}^{\delta}_{1,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[Q_Y]_\gamma} : Q_{Y^n}(y^n) < Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right\}, \\
\mathcal{B}^{\delta}_{2,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[Q_Y]_\gamma} : Q_{Y^n}(y^n) \geq Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right\}, \\
\mathcal{C}^{\delta}_{2,\gamma} &:= \left\{y^n \in \mathcal{T}^n_{[Q_Y]_\gamma} : Q_{Y^n}(y^n) < Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right\}.
\end{aligned}
$$

Then, we can write

$$
\left\|Q_{Y^n}(\cdot) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|1)\right\|
$$

$$
\begin{aligned}
&= \frac{1}{2}\sum_{y^n}\left|Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right| \\
&= \frac{1}{2}\sum_{y^n\notin\mathcal{T}^n_{[Q_Y]_\gamma}}\left|Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right| + \frac{1}{2}\sum_{y^n\in\mathcal{T}^n_{[Q_Y]_\gamma}}\left|Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right| \\
&\leq \frac{1}{2}\sum_{y^n\notin\mathcal{T}^n_{[Q_Y]_\gamma}} Q_{Y^n}(y^n) + Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) + \frac{1}{2}\sum_{y^n\in\mathcal{T}^n_{[Q_Y]_\gamma}}\left|Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right|. \qquad \text{(A4)}
\end{aligned}
$$

Next, note that

$$
Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) = Q_{Y^n}(y^n)\,\frac{Q_{\Pi(X^n,\delta,P_X)|Y^n}(1|y^n)}{Q_{\Pi(X^n,\delta,P_X)}(1)} \leq \frac{Q_{Y^n}(y^n)}{Q_{\Pi(X^n,\delta,P_X)}(1)} \leq 2Q_{Y^n}(y^n), \qquad \text{(A5)}
$$

for sufficiently large n (depending on $|\mathcal{X}|$), since $Q_{\Pi(X^n,\delta,P_X)}(1) \xrightarrow{(n)} 1$. Thus, for n large enough,

$$
\sum_{y^n\notin\mathcal{T}^n_{[Q_Y]_\gamma}} Q_{Y^n}(y^n) + Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) \leq 3\sum_{y^n\notin\mathcal{T}^n_{[Q_Y]_\gamma}} Q_{Y^n}(y^n) \leq e^{-n\Omega(\gamma)}. \qquad \text{(A6)}
$$

We can bound the last term in (A4) as follows:

$$
\begin{aligned}
&\sum_{y^n\in\mathcal{T}^n_{[Q_Y]_\gamma}}\left|Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)\right| \\
&= \sum_{y^n\in\mathcal{B}^\delta_{2,\gamma}} Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) + \sum_{y^n\in\mathcal{C}^\delta_{2,\gamma}} Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) - Q_{Y^n}(y^n) \\
&= \sum_{y^n\in\mathcal{B}^\delta_{2,\gamma}} Q_{Y^n}(y^n) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) + \sum_{y^n\in\mathcal{C}^\delta_{2,\gamma}} Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1) - Q_{Y^n}(y^n) \\
&= \sum_{y^n\in\mathcal{B}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(1 - \frac{Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)}{Q_{Y^n}(y^n)}\right) + \sum_{y^n\in\mathcal{C}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(\frac{Q_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|1)}{Q_{Y^n}(y^n)} - 1\right) \qquad \text{(A7)} \\
&= \sum_{y^n\in\mathcal{B}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(1 - \frac{Q_{\Pi(X^n,\delta,P_X)|Y^n}(1|y^n)}{Q_{\Pi(X^n,\delta,P_X)}(1)}\right) + \sum_{y^n\in\mathcal{C}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(\frac{Q_{\Pi(X^n,\delta,P_X)|Y^n}(1|y^n)}{Q_{\Pi(X^n,\delta,P_X)}(1)} - 1\right) \\
&\leq \sum_{y^n\in\mathcal{B}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(1 - Q_{\Pi(X^n,\delta,P_X)|Y^n}(1|y^n)\right) + \sum_{y^n\in\mathcal{C}^\delta_{2,\gamma}} Q_{Y^n}(y^n)\left(\frac{1}{Q_{\Pi(X^n,\delta,P_X)}(1)} - 1\right). \qquad \text{(A8)}
\end{aligned}
$$

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

$$
E_n(\delta,\gamma) := \min_{P_{\tilde{Y}}\in\mathcal{P}_n\left(\mathcal{T}^n_{[Q_Y]_\gamma}\right)}\ \min_{P_{\tilde{X}}\in\mathcal{P}_n\left(\mathcal{T}^n_{[P_X]_\delta}\right)} D(P_{\tilde{X}|\tilde{Y}}||Q_{X|Y}|P_{\tilde{Y}}).
$$

Then, for $y^n \in \mathcal{T}^n_{[Q_Y]_\gamma}$, arbitrary $\tilde{\gamma} > 0$ and n sufficiently large (depending on $|\mathcal{X}|, |\mathcal{Y}|, \delta, \gamma$), it follows from ([60], Lemma 2.6) that

$$
Q_{\Pi(X^n,\delta,P_X)|Y^n}(1|y^n) \geq 1 - e^{-n(E_n(\delta,\gamma)-\tilde{\gamma})}, \qquad \text{(A9)}
$$

$$
\text{and } Q_{\Pi(X^n,\delta,P_X)}(1) \geq 1 - e^{-n(D(P_X||Q_X)-\tilde{\gamma})}. \qquad \text{(A10)}
$$

From (A4), (A6) and (A8)–(A10), it follows that

$$\|Q_{Y^n}(\cdot) - Q_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|1)\| \leq e^{-n\Omega(\gamma)} + e^{-n(E_n(\delta,\gamma)-\tilde{\gamma})} + e^{-n(D(P_X||Q_X)-\tilde{\gamma})}. \tag{A11}$$

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 (A11) converges exponentially to zero (for $\tilde{\gamma}$ small enough) with exponent $\bar{\delta} := \min\left(\Omega(\gamma), E_n(\delta,\gamma) - \tilde{\gamma}, D(P_X||Q_X) - \tilde{\gamma}\right)$, thus proving (15). We can write,

$$E_n(\delta,\gamma) \geq \min_{P_{\tilde{Y}} \in \mathcal{T}^n_{[Q_Y]_\gamma}} \min_{P_{\tilde{X}} \in \mathcal{T}^n_{[P_X]_\delta}} D(P_{\tilde{X}}||\hat{Q}_X) \tag{A12}$$

$$\geq 2\left[\min_{P_{\tilde{Y}} \in \mathcal{T}^n_{[Q_Y]_\gamma}} \min_{P_{\tilde{X}} \in \mathcal{T}^n_{[P_X]_\delta}} \|P_{\tilde{X}} - \hat{Q}_X\|^2\right], \tag{A13}$$

where

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

Here, (A12) follows due to the convexity of KL divergence (A13) is due to Pinsker's inequality [60]. We also have from the triangle inequality satisfied by 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 $y^n \in \mathcal{T}^n_{[Q_Y]_\gamma}$,

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

Also, for $P_{\tilde{X}} \in \mathcal{T}^n_{[P_X]_\delta}$,

$$\|P_{\tilde{X}} - P_X\| \leq O(\delta).$$

Hence,

$$E_n(\delta,\gamma) \geq 2\left(\|P_X - Q_X\| - O(\gamma) - O(\delta)\right)^2.$$

Since $P_X \neq Q_X$, $E_n(\delta,\gamma) > 0$ for sufficiently small $\gamma > 0$ and $\delta > 0$. This completes the proof of (15).
We next prove (17). Similar to (A4) and (A5), we have,

$$\begin{aligned}&\left\|P_{Y^n}(\cdot) - P_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|0)\right\| \\ &\leq \frac{1}{2}\sum_{y^n \notin \mathcal{T}^n_{[P_Y]_\gamma}} \left[P_{Y^n}(y^n) + P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right] + \frac{1}{2}\sum_{y^n \in \mathcal{T}^n_{[P_Y]_\gamma}} \left|P_{Y^n}(y^n) - P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0)\right|,\end{aligned} \tag{A14}$$

and

$$P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0) \leq 2P_{Y^n}(y^n), \tag{A15}$$

since $P_{\Pi(X^n,\delta,P_X)}(0) \xrightarrow{(n)} 1$.

Also, for $\gamma < \frac{\delta}{|\mathcal{Y}|}$ and sufficiently large n (depending on $\delta, \gamma, |\mathcal{X}|, |\mathcal{Y}|$), we have

$$\begin{aligned}
&\sum_{y^n \in \mathcal{T}^n_{[P_Y]_\gamma}} \left| P_{Y^n}(y^n) - P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0) \right| \\
&= \sum_{y^n \in \mathcal{B}^\delta_{0,\gamma}} P_{Y^n}(y^n) - P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0) + \sum_{y^n \in \mathcal{C}^\delta_{0,\gamma}} P_{Y^n|\Pi(X^n,\delta,P_X)}(y^n|0) - P_{Y^n}(y^n) \\
&\leq \sum_{y^n \in \mathcal{B}^\delta_{0,\gamma}} P_{Y^n}(y^n) \left(1 - P_{\Pi(X^n,\delta,P_X)|Y^n}(0|y^n)\right) + \sum_{y^n \in \mathcal{C}^\delta_{0,\gamma}} P_{Y^n}(y^n) \left(\frac{1}{P_{\Pi(X^n,\delta,P_X)}(0)} - 1\right) \\
&\leq \sum_{y^n \in \mathcal{B}^\delta_{0,\gamma}} P_{Y^n}(y^n) e^{-n\Omega(\delta-\gamma|\mathcal{Y}|)} + \sum_{y^n \in \mathcal{C}^\delta_{0,\gamma}} P_{Y^n}(y^n) e^{-n\Omega(\delta)} \qquad \text{(A16)} \\
&\leq e^{-n\Omega(\delta-\gamma|\mathcal{Y}|)}, \qquad \text{(A17)}
\end{aligned}$$

where to obtain (A16), we used

$$P_{\Pi(X^n,\delta,P_X)}(0) \geq 1 - e^{-n\Omega(\delta)}, \qquad \text{(A18)}$$

$$\text{and } P_{\Pi(X^n,\delta,P_X)|Y^n}(0|y^n) \geq 1 - e^{-n\Omega(\delta-\gamma|\mathcal{Y}|)}, \text{ for } y^n \in \mathcal{B}^\delta_{0,\gamma} \text{ and } \gamma < \frac{\delta}{|\mathcal{Y}|}. \qquad \text{(A19)}$$

Here, (A18) follows from ([60], Lemma 2.12), and (A19) follows from ([60], Lemmas 2.10 and 2.12), respectively. Thus, from (A14), (A15) and (A17), we can write that,

$$\left\| P_{Y^n}(\cdot) - P_{Y^n|\Pi(X^n,\delta,P_X)}(\cdot|0) \right\| \leq e^{-n\Omega(\gamma)} + e^{-n\Omega(\delta-\gamma|\mathcal{Y}|)} \xrightarrow{(n)} 0.$$

This completes the proof of (17). The proof of (16) is exactly the same as (17), with the only difference that the sets $\mathcal{B}^\delta_{1,\gamma}$ and $\mathcal{C}^\delta_{1,\gamma}$ are used in place of $\mathcal{B}^\delta_{0,\gamma}$ and $\mathcal{C}^\delta_{0,\gamma}$, respectively.

Appendix D. Proof of Theorems 1 and 2

We describe the encoding and decoding operations which are the same for both Theorems 1 and 2. Fix positive numbers (small) $\eta, \delta > 0$, and let $\delta' := \frac{\delta}{2}$, $\hat{\delta} := |\mathcal{U}|\delta$, $\tilde{\delta} := 2\delta$ and $\bar{\delta} := \frac{\delta'}{|\mathcal{V}|}$.

Codebook Generation: Fix a finite alphabet $\mathcal{W}$ and a conditional distribution $P_{W|U}$. Let $\mathbb{B}_n = \{W^n(j),\ j \in [M'_n]\}$, $M'_n := e^{n(I_P(U:W)+\eta)}$, denote a random codebook such that each $W^n(j)$ is randomly and independently generated according to distribution $\prod_{i=1}^n P_W(w_i)$, where

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

Denote a realization of $\mathbb{B}_n$ by $\mathcal{B}_n$ and the support of $\mathbb{B}_n$ by $\mathfrak{B}_n$.

Encoding: For a given codebook $\mathcal{B}_n$, let

$$P^{(\mathcal{B}_n)}_{\mathsf{E_u}}(j|u^n) := \frac{\prod_{i=1}^n P_{U|W}(u_i|w_i(j))}{\sum_{j'} \prod_{i=1}^n P_{U|W}(u_i|w_i(j')))}, \qquad \text{(A20)}$$

denote the likelihood encoding function. If $I_P(U;W) + \eta + |\mathcal{U}||\mathcal{W}|\frac{\log(n+1)}{n} > R$, the observer performs uniform random binning on the indices in $[M'_n]$, i.e., for each $j \in [M'_n]$, it selects an index uniformly at random from the set $\tilde{\mathcal{M}}_n := \left[e^{n\left(R - |\mathcal{U}||\mathcal{W}|\frac{\log(n+1)}{n}\right)}\right]$. Denote the random binning function by $f_{\mathbb{B}}$ and

a realization of it by f_{B}. If $I_P(U;W)+\eta+|\mathcal{U}||\mathcal{W}|\frac{\log(n+1)}{n} \leq R$, set $f_{\mathbb{B}}$ as the identity function with probability one, i.e., $f_{\mathbb{B}}(j)=j$. If $u^n \in \mathcal{T}^n_{[P_U]_{\delta'}}$, then the observer outputs the message $m=(t, f_{\mathsf{B}}(j))$ if $I_P(U;W)+\eta+|\mathcal{U}||\mathcal{W}|\frac{\log(n+1)}{n} > R$ or $m=(t,j)$ otherwise, where $j \in [M'_n]$ is chosen randomly with probability $P_{\mathsf{E_u}}^{(\mathcal{B}_n)}(j|u^n)$ and t denotes the index of the joint type of $(u^n, w^n(j))$ in the set of types $\mathcal{P}^n(\mathcal{U}\times\mathcal{W})$. If $u^n \notin \mathcal{T}^n_{[P_U]_{\delta'}}$, the observer outputs the *error* message $M=0$. Please note that $|\mathcal{M}| \leq e^{nR}$ since the total number of types in $\mathcal{P}^n(\mathcal{U}\times\mathcal{W})$ is upper bounded by $(n+1)^{|\mathcal{U}||\mathcal{W}|}$ ([60], Lemma 2.2). Let $\mathbb{C}_n := (\mathbb{B}_n, f_{\mathbb{B}})$, and let $\mathcal{C}_n = (\mathcal{B}_n, f_{\mathsf{B}})$ and $\mu_n(\cdot)$ denote its realization and probability distribution, respectively. For a given $\mathcal{C}_n$, let $f_n^{(\mathcal{C}_n)}$ represent the encoder induced by the above operations, where $f_n^{(\mathcal{C}_n)} : \mathcal{U}^n \to \mathcal{P}(\mathcal{M})$ and $\mathcal{M} := [e^{nR}]$.

Decoding: If $M=0$ or $t \notin \mathcal{T}^n_{[P_{UW}]_\delta}$, $\hat{H}=1$ is declared. Else, given $m=(t, f_{\mathsf{B}}(j))$ and $V^n=v^n$, the detector decodes for a codeword $\hat{w}^n := w^n(\hat{j}) \in \mathcal{T}^n_{[P_W]_\delta}$ in the codebook $\mathcal{B}_n$ such that

$$\hat{j} = \underset{\substack{l:\, f_{\mathsf{B}}(l)=f_{\mathsf{B}}(j),\\ w^n(l)\in\mathcal{T}^n_{[P_W]_\delta}}}{\arg\min} H_e(w^n(l)|v^n), \text{ if } I_P(U;W)+\eta+\frac{1}{n}|\mathcal{U}||\mathcal{W}|\log(n+1) > R,$$

$$\hat{j} = j, \text{ otherwise.}$$

Denote the above decoding rule by $P_{\mathsf{ED}}^{(\mathcal{C}_n)}$, where $P_{\mathsf{ED}}^{(\mathcal{C}_n)} : \mathcal{M}\times\mathcal{V}^n \to \mathcal{J}$. The detector declares $\hat{H}=0$ if $(\hat{w}^n, v^n) \in \mathcal{T}^n_{[P_{WV}]_\delta}$ and $\hat{H}=1$ otherwise. Let $g_n^{(\mathcal{C}_n)} : \mathcal{M}\times\mathcal{V}^n \to \hat{\mathcal{H}}$ stand for the decision rule induced by the above operations.

System induced distributions and auxiliary distributions:

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

$$\begin{aligned}
&\tilde{P}^{(\mathcal{C}_n,0)}(s^n,u^n,v^n,j,w^n,m,\hat{j},\hat{w}^n)\\
&= \left[\prod_{i=1}^n P_{SUV}(s_i,u_i,v_i,z_i)\right] P_{\mathsf{E_u}}^{(\mathcal{B}_n)}(j|u^n)\mathbb{1}(w^n(j)=w^n)\mathbb{1}(f_{\mathsf{B}}(j)=m)\ \mathbb{1}\left(\hat{j}=P_{\mathsf{ED}}^{(\mathcal{C}_n)}(m,v^n)\right)\\
&\quad \mathbb{1}(w^n(\hat{j})=\hat{w}^n), \qquad\qquad \text{if } u^n \in \mathcal{T}^n_{[P_U]_{\delta'}},
\end{aligned} \tag{A21}$$

and

$$\tilde{P}^{(\mathcal{C}_n,0)}(s^n,u^n,v^n,m) = \left[\prod_{i=1}^n P_{SUV}(s_i,u_i,v_i)\right]\mathbb{1}(m=0), \qquad \text{if } u^n \notin \mathcal{T}^n_{[P_U]_{\delta'}}. \tag{A22}$$

Consider two auxiliary distribution $\tilde{\Psi}$ and Ψ given by

$$\begin{aligned}
&\tilde{\Psi}^{(\mathcal{C}_n,0)}(s^n,u^n,v^n,j,w^n,m,\hat{j},\hat{w}^n)\\
&:= \left[\prod_{i=1}^n P_{SUV}(s_i,u_i,v_i)\right] P_{\mathsf{E_u}}^{(\mathcal{B}_n)}(j|u^n)\mathbb{1}(w^n(j)=w^n)\mathbb{1}(f_{\mathsf{B}}(j)=m)\ \mathbb{1}\left(\hat{j}=P_{\mathsf{ED}}^{(\mathcal{C}_n)}(m,v^n)\right)\\
&\qquad \mathbb{1}(w^n(\hat{j})=\hat{w}^n),
\end{aligned} \tag{A23}$$

and

$$\Psi^{(\mathcal{C}_n,0)}(s^n,u^n,v^n,j,w^n,m,\hat{j},\hat{w}^n)$$

$$:= \frac{1}{M'_n}\, \mathbb{1}(w^n(j) = w^n) \left[\prod_{i=1}^{n} P_{U|W}(u_i|w_i)\right] \left[\prod_{i=1}^{n} P_{VS|U}(v_i, s_i|u_i)\right] \mathbb{1}(f_{\mathsf{B}}(j) = m)\, \mathbb{1}\left(\hat{j} = P_{\mathsf{ED}}^{(\mathcal{C}_n)}(m, v^n)\right) \mathbb{1}(w^n(\hat{j}) = \hat{w}^n). \tag{A24}$$

Let $\tilde{P}^{(\mathcal{C}_n,1)}$ and $\tilde{\Psi}^{(\mathcal{C}_n,1)}$ denote probability distributions under $H = 1$ defined by the R.H.S. of (A21)–(A23) with P_{SUV} replaced by Q_{SUV}, and let $\Psi^{(\mathcal{C}_n,1)}$ denote the R.H.S. of (A24) with $P_{VS|U}$ replaced by $Q_{VS|U}$. Please note that the encoder $f_n^{(\mathcal{C}_n)}$ is such that $P_{\mathsf{E_u}}^{(\mathcal{B}_n)}(j|u^n) = \Psi^{(\mathcal{C}_n,0)}(j|u^n)$ and hence, the only difference between the joint distribution $\Psi^{(\mathcal{C}_n,0)}$ and $\tilde{\Psi}^{(\mathcal{C}_n,0)}$ is the marginal distribution of U^n. By the soft-covering lemma [62,64], it follows that for some $\gamma_1 > 0$,

$$\mathbb{E}_{\mu_n}\left[\left\|\Psi_{U^n}^{(\mathbb{C}_n,0)} - \tilde{\Psi}_{U^n}^{(\mathbb{C}_n,0)}\right\|\right] \leq e^{-n\gamma_1} \xrightarrow{(n)} 0. \tag{A25}$$

Hence, from ([43], Property 2(d)), it follows that

$$\mathbb{E}_{\mu_n}\left[\left\|\Psi^{(\mathbb{C}_n,0)} - \tilde{\Psi}^{(\mathbb{C}_n,0)}\right\|\right] \leq e^{-n\gamma_1}. \tag{A26}$$

Also, note that the only difference between the distributions $\tilde{P}^{(\mathcal{C}_n,0)}$ and $\tilde{\Psi}^{(\mathcal{C}_n,0)}$ is $P_{\mathsf{E_u}}^{(\mathcal{B}_n)}$ when $U^n \notin \mathcal{T}^n_{[P_U]_{\delta'}}$. Since

$$\mathbb{P}\left(U^n \notin \mathcal{T}^n_{[P_U]_{\delta'}} | H = 0\right) \leq e^{-n\Omega(\delta')}, \tag{A27}$$

it follows that

$$\mathbb{E}_{\mu_n}\left[\left\|\tilde{P}^{(\mathbb{C}_n,0)} - \tilde{\Psi}^{(\mathbb{C}_n,0)}\right\|\right] \leq e^{-n\Omega(\delta')}. \tag{A28}$$

Equations (A26) and (A28) together imply via ([43], Property 2(c)) that

$$\mathbb{E}_{\mu_n}\left[\left\|\tilde{P}^{(\mathbb{C}_n,0)} - \Psi^{(\mathbb{C}_n,0)}\right\|\right] \leq e^{-n\Omega(\delta')} + e^{-n\gamma_1} \xrightarrow{(n)} 0. \tag{A29}$$

Please note that for $l \in \{0, 1\}$, the joint distribution $\Psi^{(\mathcal{C}_n,l)}$ satisfies

$$S_i - (w_i(J), V_i) - (M, w^n(J), V^n, S^{i-1}),\ i \in [n]. \tag{A30}$$

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

$$\mathbb{E}_{\mu_n}\left[\sum_{i=1}^{n} \left\|P_W - \Psi_{W_i(J)}^{(\mathbb{C}_n,l)}\right\| \,\middle|\, H = l\right] \leq e^{-\gamma_3 n} \xrightarrow{(n)} 0,\ l = 0, 1, \tag{A31}$$

for some $\gamma_3 > 0$.

If $Q_U = P_U$, then it again follows from the soft-covering lemma that

$$\mathbb{E}_{\mu_n}\left[\left\|\Psi_{U^n}^{(\mathbb{C}_n,1)} - \tilde{\Psi}_{U^n}^{(\mathbb{C}_n,1)}\right\|\right] \leq e^{-\gamma_1 n} \xrightarrow{(n)} 0, \tag{A32}$$

thereby implying that

$$\mathbb{E}_{\mu_n}\left[\left\|\Psi^{(\mathbb{C}_n,1)} - \tilde{\Psi}^{(\mathbb{C}_n,1)}\right\|\right] \leq e^{-\gamma_1 n}. \tag{A33}$$

Also, note that the only difference between the distributions $\tilde{P}^{(\mathcal{C}_n,1)}$ and $\tilde{\Psi}^{(\mathcal{C}_n,1)}$ is $P_{\mathsf{E_u}}^{(\mathcal{B}_n)}$ when $U^n \notin \mathcal{T}^n_{[P_U]_{\delta'}}$. Since $Q_U = P_U$ implies $\mathbb{P}\left(U^n \notin \mathcal{T}^n_{[P_U]_{\delta'}} \middle| H = 1\right) \leq e^{-n\Omega(\delta')}$, it follows that

$$\mathbb{E}_{\mu_n}\left[\left\|\tilde{P}^{(\mathbb{C}_n,1)} - \tilde{\Psi}^{(\mathbb{C}_n,1)}\right\|\right] \leq e^{-n\Omega(\delta')}. \tag{A34}$$

Equations (A33) and (A34) together imply that

$$\mathbb{E}_{\mu_n}\left[\left\|\tilde{P}^{(\mathbb{C}_n,1)} - \Psi^{(\mathbb{C}_n,1)}\right\|\right] \leq e^{-n\Omega(\delta')} + e^{-\gamma_1 n} \xrightarrow{(n)} 0. \tag{A35}$$

Let $\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}} = \mathbb{E}_{\mu_n}\left[\mathbb{P}_{\tilde{P}^{(\mathbb{C}_n,0)}}\right]$ and $\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,1)}} = \mathbb{E}_{\mu_n}\left[\mathbb{P}_{\tilde{P}^{(\mathbb{C}_n,1)}}\right]$ denote the expected probability measure (random coding measure) induced by PMF's $\tilde{P}^{(\mathbb{C}_n,0)}$ and $\tilde{P}^{(\mathbb{C}_n,1)}$, respectively. Then, note that from (A24), (A29), (A31) and the weak law of large numbers,

$$\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}\left(\left(U^n, W^n(J)\right) \in \mathcal{T}^n_{[P_{UW}]_\delta}\right) \geq 1 - e^{-n\Omega(\delta)} \xrightarrow{(n)} 1. \tag{A36}$$

Analysis of type I and type II error probabilities:
We analyze type I and type II error probabilities of the coding scheme mentioned above averaged over the random ensemble $\mathbb{C}_n$.
Type I error probability:
Please note that a type I error occurs only if one of the following events occur:

$$\begin{aligned}
\mathcal{E}_{\mathsf{TE}} &= \left\{(U^n, V^n) \notin \mathcal{T}^n_{[P_{UV}]_\delta}\right\},\\
\mathcal{E}_{\mathsf{SE}} &= \left\{T \notin \mathcal{P}_n\left(\mathcal{T}^n_{[P_{UW}]_\delta}\right)\right\},\\
\mathcal{E}_{\mathsf{ME}} &= \left\{\left(V^n, W^n(J)\right) \notin \mathcal{T}^n_{[P_{VW}]_\delta}\right\},\\
\mathcal{E}_{\mathsf{DE}} &= \Big\{\exists\, l \in \left[e^{n(I_P(U;W)+\eta)}\right],\ l \neq J : f_{\mathbb{B}}(l) = f_{\mathbb{B}}(J),\ W^n(l) \in \mathcal{T}^n_{[P_W]_\delta},\\
&\qquad H_e\left(W^n(l)|V^n\right) \leq H_e\left(W^n(J)|V^n\right)\Big\}.
\end{aligned}$$

Let $\mathcal{E} := \mathcal{E}_{\mathsf{TE}} \cup \mathcal{E}_{\mathsf{SE}} \cup \mathcal{E}_{\mathsf{ME}} \cup \mathcal{E}_{\mathsf{DE}}$. Then, the expected type I error probability over $\mathbb{C}_n$ be upper bounded as

$$\mathbb{E}_{\mu_n}\left[\alpha_n\left(f_n^{(\mathbb{C}_n)}, g_n^{(\mathbb{C}_n)}\right)\right] \leq \bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}(\mathcal{E}). \tag{A37}$$

Please note that $\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}(\mathcal{E}_{\mathsf{TE}})$ tends to 0 asymptotically by the weak law of large numbers. From (A36), $\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}(\mathcal{E}_{\mathsf{SE}}) \xrightarrow{(n)} 0$. Given $\mathcal{E}^c_{\mathsf{SE}}$ and $\mathcal{E}^c_{\mathsf{TE}}$ holds, it follows from the Markov chain relation $V - U - W$ and the Markov lemma [68] that $\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}(\mathcal{E}_{\mathsf{ME}}) \xrightarrow{(n)} 0$. Also, as in the proof of Theorem 2 in [13], it follows that

$$\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,0)}}(\mathcal{E}_{\mathsf{DE}}|\ V^n = v^n, W^n(J) = w^n, \mathcal{E}^c_{\mathsf{ME}} \cap \mathcal{E}^c_{\mathsf{SE}} \cap \mathcal{E}^c_{\mathsf{TE}}) \leq e^{-n\left(R - I_P(U;W|V) - \delta_n^{(1)}\right)}, \tag{A38}$$

where $\delta_n^{(1)} \xrightarrow{(n)} \eta + O(\delta)$. Thus, if $R > I_P(U;W|V)$, it follows by choosing $\eta = O(\delta)$ that for $\delta > 0$ small enough, the R.H.S. of (A38) tends to zero asymptotically. By the union bound on probability, the R.H.S. of (A37) tends to zero.

Type II error probability:

Let $\delta'' = |\mathcal{W}|\tilde{\delta}$. Please note that a type II error occurs only if $V^n \in \mathcal{T}^n_{[P_V]_{\delta''}}$ and $M \neq 0$, i.e., $U^n \in \mathcal{T}^n_{[P_U]_{\delta'}}$ and $T \in \mathcal{T}^n_{[P_{UW}]_{\delta}}$. Hence, we can restrict the type II error analysis to only such (U^n, V^n). Denoting the event that a type II error occurs by $\mathcal{D}_0$, we have

$$\mathbb{E}_{\mu_n}\left[\beta_n\left(f_n^{(\mathbb{C}_n)}, g_n^{(\mathbb{C}_n)}\right)\right] = \sum_{u^n, v^n} \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(U^n = u^n, V^n = v^n)\, \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | U^n = u^n, V^n = v^n). \tag{A39}$$

Let $\mathcal{E}_{\mathsf{NE}} := \mathcal{E}^c_{\mathsf{SE}} \cap \left\{V^n \in \mathcal{T}^n_{[V]_{\delta''}}\right\} \cap \left\{U^n \in \mathcal{T}^n_{[U]_{\delta'}}\right\}$. The last term in (A39) can be upper bounded as follows:

$$\begin{aligned}
&\bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | U^n = u^n, V^n = v^n) \\
&= \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{NE}} | U^n = u^n, V^n = v^n)\, \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{\mathsf{NE}}) \\
&\leq \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, \mathcal{E}_{\mathsf{NE}}) \\
&= \sum_{j,\tilde{m}} \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(J = j, f_{\mathbb{B}}(J) = \tilde{m} | U^n = u^n, V^n = v^n, \mathcal{E}_{\mathsf{NE}}) \\
&\qquad \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 |\, U^n = u^n, V^n = v^n, J = j, f_{\mathbb{B}}(J) = \tilde{m}, \mathcal{E}_{\mathsf{NE}}) &\text{(A40)} \\
&= \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 |\, U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1, \mathcal{E}_{\mathsf{NE}}) &\text{(A41)} \\
&= \sum_{w^n \in \mathcal{W}^n} \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1,\ \mathcal{E}_{\mathsf{NE}}) \\
&\qquad \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1, W^n(1) = w^n,\ \mathcal{E}_{\mathsf{NE}}). &\text{(A42)}
\end{aligned}$$

where (A41) follows since the term in (A40) is independent of the indices $(j, \tilde{m})$ due to the symmetry of the codebook generation, encoding and decoding procedure. The first term in (A42) can be upper bounded as

$$\begin{aligned}
&\bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(W^n(1) = w^n | U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1,\ \mathcal{E}_{\mathsf{NE}}) \\
&\leq \frac{1}{|\mathcal{T}_{P_{\tilde{W}|\tilde{U}}}|} \leq e^{-n(H(\tilde{W}|\tilde{U}) - \frac{1}{n}|\mathcal{U}||\mathcal{W}|\log(n+1))}.
\end{aligned} \tag{A43}$$

To obtain (A43), we used the fact that $P_{\mathsf{E_u}}^{(\mathcal{B}_n)}(1|u^n)$ in (A20) is invariant to the joint type $P_{\tilde{U}\tilde{W}}$ of $(U^n, W^n(1)) = (u^n, w^n)$ (keeping all the other codewords fixed). This in turn implies that given $\mathcal{E}_{\mathsf{NE}}$, each sequence in the conditional type class $\mathcal{T}_{P_{\tilde{W}|\tilde{U}}}(u^n)$ is equally likely (in the randomness induced by $\mathbb{B}_n$ and stochastic encoding in (A20)) and its probability is upper bounded by $\frac{1}{|\mathcal{T}_{P_{\tilde{W}|\tilde{U}}}|}$. Defining the events

$$\mathcal{E}_{\mathsf{BE}} := \left\{\exists\, l \in \left[M_n'\right],\, l \neq J,\, f_{\mathbb{B}}(l) = M,\, W^n(l)) \in \mathcal{T}^n_{[P_W]_{\tilde{\delta}}}, (V^n, W^n(l)) \in \mathcal{T}^n_{[P_{VW}]_{\tilde{\delta}}}\right\}, \tag{A44}$$

$$\mathcal{F} := \{U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1, W^n(1) = w^n,\ \mathcal{E}_{\mathsf{NE}}\}, \tag{A45}$$

$$\mathcal{F}_1 := \{U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1, W^n(1) = w^n,\ \mathcal{E}_{\mathsf{NE}},\ \mathcal{E}^c_{\mathsf{BE}}\}, \tag{A46}$$

$$\text{and } \mathcal{F}_2 := \{U^n = u^n, V^n = v^n, J = 1, f_{\mathbb{B}}(J) = 1, W^n(1) = w^n,\ \mathcal{E}_{\mathsf{NE}},\ \mathcal{E}_{\mathsf{BE}}\}, \tag{A47}$$

the last term in (A42) can be written as

$$\bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | \mathcal{F}) = \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{E}^c_{\mathsf{BE}} | \mathcal{F})\, \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | \mathcal{F}_1) + \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{BE}} | \mathcal{F})\, \bar{\mathbb{P}}_{\tilde{p}(\mathbb{C}_n,1)}(\mathcal{D}_0 | \mathcal{F}_2). \tag{A48}$$

The analysis of the terms in (A48) is essentially similar to that given in the proof of Theorem 2 in [13], except for a subtle difference that we mention next. To bound the *binning* error event $\mathcal{E}_{\mathsf{BE}}$, we require an upper bound similar to

$$\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}\left(W^n(l)=\tilde{w}^n|\mathcal{F}\right) \leq 2\,\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(l)=\tilde{w}^n),\ \forall\ \tilde{w}^n \in \mathcal{W}^n, \tag{A49}$$

that is used in the proof of Theorem 2 in [13]. Please note that the stochastic encoding scheme considered here is different from the encoding scheme in [13]. In place (A49), we will show that for $l \neq 1$,

$$\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(l)=\tilde{w}^n|\ \mathcal{F}) \leq 3\,\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(l)=\tilde{w}^n), \tag{A50}$$

which suffices for the proof. Please note that

$$\begin{aligned}
&\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(l)=\tilde{w}^n|\mathcal{F})\\
&=\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(l)=\tilde{w}^n|U^n=u^n,V^n=v^n)\frac{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(1)=w^n|W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)}{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(1)=w^n|U^n=u^n,V^n=v^n)}\\
&\quad\frac{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(J=1|W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)}{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(J=1|W^n(1)=w^n,U^n=u^n,V^n=v^n)} \qquad \text{(A51)}\\
&\quad\frac{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(f_{\mathbb{B}}(J)=1|J=1,W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)}{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(f_{\mathbb{B}}(J)=1|J=1,W^n(1)=w^n,U^n=u^n,V^n=v^n)}\\
&\quad\frac{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{NE}}|f_{\mathbb{B}}(J)=1,J=1,W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)}{\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{NE}}|f_{\mathbb{B}}(J)=1,J=1,W^n(1)=w^n,U^n=u^n,V^n=v^n)} \qquad \text{(A52)}
\end{aligned}$$

Since the codewords are generated independently of each other and the binning operation is done independent of the codebook generation, we have

$$\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(1)=w^n|W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)=\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(W^n(1)=w^n|U^n=u^n,V^n=v^n), \tag{A53}$$

and

$$\begin{aligned}
&\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(f_{\mathbb{B}}(J)=1|J=1,W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)\\
&=\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(f_{\mathbb{B}}(J)=1|J=1,W^n(1)=w^n,U^n=u^n,V^n=v^n).
\end{aligned} \tag{A54}$$

Also, note that

$$\begin{aligned}
&\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{NE}}|f_{\mathbb{B}}(J)=1,J=1,W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n)\\
&=\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(\mathcal{E}_{\mathsf{NE}}|f_{\mathbb{B}}(J)=1,J=1,W^n(1)=w^n,U^n=u^n,V^n=v^n).
\end{aligned} \tag{A55}$$

Next, consider the term in (A51). Let

$$\begin{aligned}
\mathcal{F}' &:= \{W^n(1)=w^n,U^n=u^n,V^n=v^n\},\\
\mathcal{F}'' &:= \{W^n(1)=w^n,W^n(l)=\tilde{w}^n,U^n=u^n,V^n=v^n\}.
\end{aligned}$$

Then, the numerator and denominator of (A51) can be written as

$$\bar{\mathbb{P}}_{\tilde{P}(\mathbb{C}_n,1)}(J=1|\mathcal{F}'')$$

$$= \mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\prod_{i=1}^n P_{U|W}(u_i|\tilde{w}_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]$$
$$\leq \mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right], \tag{A56}$$

and

$$\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,1)}}(J=1|\mathcal{F}') = \mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right], \tag{A57}$$

respectively. The R.H.S. of (A56) (resp. (A57)) denote the average probability that $J=1$ is chosen by $P_{\mathsf{E}_u}^{(\mathbb{B}_n)}$ given $W^n(1)=w^n$, $U^n=u^n$ and $M_n'-2$ (resp. $M_n'-1$) other independent codewords in $\mathbb{B}_n$. Let

$$\mathcal{E}_l := \left\{\prod_{i=1}^n P_{U|W}(u_i|W_i(l)) \geq \max\left(\left\{\prod_{i=1}^n P_{U|W}(u_i|W_i(j)),\ j\in\lceil M_n'\rceil\backslash\{1\}\right\}\cup\left\{\prod_{i=1}^n P_{U|W}(u_i|w_i)\right\}\right)\right\}.$$

Please note that

$$\mathbb{E}_{\mu_n|\mathcal{E}_l^c}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]$$
$$\geq \frac{1}{2}\mathbb{E}_{\mu_n|\mathcal{E}_l^c}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]. \tag{A58}$$

Hence, denoting by $\bar{\mu}_n$ the probability measure induced by μ_n, we have

$$\frac{\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,1)}}(J=1|\mathcal{F}'')}{\bar{\mathbb{P}}_{\tilde{P}^{(\mathbb{C}_n,1)}}(J=1|\mathcal{F}')}$$
$$\leq \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}$$
$$\leq \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}{\bar{\mu}_n(\mathcal{E}_l^c)\mathbb{E}_{\mu_n|\mathcal{E}_l^c}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}$$
$$\leq \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}{\frac{1}{2}\bar{\mu}_n(\mathcal{E}_l^c)\mathbb{E}_{\mu_n|\mathcal{E}_l^c}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]} \tag{A59}$$
$$= \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}{\frac{1}{2}\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]-\frac{1}{2}\bar{\mu}_n(\mathcal{E}_l)\mathbb{E}_{\mu_n|\mathcal{E}_l}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]} \tag{A60}$$
$$\leq \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]}{\frac{1}{2}\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^n P_{U|W}(u_i|w_i)}{\prod_{i=1}^n P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^n P_{U|W}(u_i|W_i(j))}\right]-\frac{1}{2}\bar{\mu}_n(\mathcal{E}_l)} \tag{A61}$$

$$\leq \frac{\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^{n} P_{U|W}(u_i|w_i)}{\prod_{i=1}^{n} P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^{n} P_{U|W}(u_i|W_i(j))}\right]}{\frac{1}{2}\mathbb{E}_{\mu_n}\left[\frac{\prod_{i=1}^{n} P_{U|W}(u_i|w_i)}{\prod_{i=1}^{n} P_{U|W}(u_i|w_i)+\sum_{j\neq 1,l}\prod_{i=1}^{n} P_{U|W}(u_i|W_i(j))}\right] - e^{-e^{n(I_P(U;W)+\eta')}}} \tag{A62}$$

$$\leq 2 + o(1) \leq 3, \tag{A63}$$

where (A59) is due to (A58); (A61) is since the term within $\mathbb{E}_{\mu_n|\mathcal{E}_l}[\cdot]$ in (A60) is upper bounded by one; (A62) is since $\bar{\mu}_n(\mathcal{E}_l) \leq e^{-e^{n(I_P(U;W)+\eta')}}$ for some $\eta' > 0$ which follows similar to ([68], Section 3.6.3), and (A63) follows since the term within the expectation which is exponential in order dominates the double exponential term. From (A52)–(A55), (A63) and (A50) follows. The analysis of the other terms in (A48) is the same as in the SHA scheme in [7], and results in the error exponent (within an additive $O(\delta)$ term) claimed in the Theorem. We refer the reader to ([13], Theorem 2) for a detailed proof (In [13], the communication channel between the observer and the detector is a DMC. However, since the coding scheme used in the achievability part of Theorem 2 in [13] is a separation-based scheme, the error exponent when the channel is noiseless can be recovered by setting $E_3(\cdot)$ and $E_4(\cdot)$ in Theorem 2 to ∞). By the random coding argument followed by the standard expurgation technique [72] (see ([13], Proof of Theorem 2)), there exists a deterministic codebook and binning function pair $\mathcal{C}_n = (\mathcal{B}_n, f_{\mathsf{B}})$ such that the type I and type II error probabilities are within a constant multiplicative factor of their average values over the random ensemble $\mathbb{C}_n$, and

$$S_i - (w_i(J), V_i) - (M, w^n(J), V^n, S^{i-1}),\ i \in [n], \tag{A64}$$

$$\left\|\tilde{P}^{(\mathcal{C}_n,0)} - \Psi^{(\mathcal{C}_n,0)}\right\| \leq e^{-\gamma_4 n}, \tag{A65}$$

$$\left\|\tilde{P}^{(\mathcal{C}_n,1)} - \Psi^{(\mathcal{C}_n,1)}\right\| \leq e^{-\gamma_4 n}, \text{ if } Q_U = P_U, \tag{A66}$$

$$\text{and } \sum_{i=1}^{n}\left\|P_W - \Psi^{(\mathcal{C}_n,l)}_{w_i(J)}\right\| \leq e^{-\gamma_5 n},\ l = 0, 1, \tag{A67}$$

where γ_4 and γ_5 are some positive numbers. Since the average type I error probability for our scheme tends to zero asymptotically, and the error exponent is unaffected by a constant multiplicative scaling of the type II error probability, this codebook achieves the same type I error probability and error exponent as the average over the random ensemble. Using this deterministic codebook for encoding and decoding, we first lower bound the equivocation and average distortion of S^n at the detector as follows:

First consider the equivocation of S^n under the null hypothesis.

$$H_{\tilde{P}(\mathcal{C}_n,0)}(S^n|M, V^n) \geq \mathbb{P}_{\tilde{P}(\mathcal{C}_n,0)}(M \neq 0) H(S^n|M \neq 0, V^n)$$

$$\geq (1 - e^{-n\Omega(\delta)})\, H_{\tilde{P}(\mathcal{C}_n,0)}(S^n|M \neq 0, V^n) \tag{A68}$$

$$\geq (1 - e^{-n\Omega(\delta)})\, H_{\tilde{P}(\mathcal{C}_n,0)}(S^n|w^n(J), V^n) \tag{A69}$$

$$= (1 - e^{-n\Omega(\delta)})\, H_{\tilde{P}(\mathcal{C}_n,0)}(S^n|w^n(J), V^n) \tag{A70}$$

$$\geq (1 - e^{-n\Omega(\delta)})\, H_{\Psi(\mathcal{C}_n,0)}(S^n|w^n(J), V^n) - 2e^{-\gamma_4 n} \log\left(\frac{|\mathcal{S}|^n|\mathcal{V}|^n}{e^{-\gamma_4 n}}\right) \tag{A71}$$

$$= \sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,0)}(S_i|w_i(J), V_i) - e^{-n\Omega(\delta)} \sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,0)}(S_i|w_i(J), V_i) - o(1) \tag{A72}$$

$$\geq \sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,0)}(S_i|w_i(J), V_i) - ne^{-n\Omega(\delta)} H_P(S|V) - o(1) \tag{A73}$$

$$= \left[\sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,0)}(S_i|w_i(J), V_i)\right] - o(1) \tag{A74}$$

$$= nH_P(S|W,V) - o(1). \tag{A75}$$

Here, (A68) follows from (A27); (A69) follows since M is a function of $w^n(J)$ for a deterministic codebook; (A71) follows from (A65) and Lemma 3; (A72) follows from (A24); and (A75) follows from (A67) and $\Psi^{(0)}_{S_iV_i|w_i} = P^{(0)}_{SV|W}$, $i \in [n]$.

If $Q_U = P_U$, it follows similarly to above that

$$H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|M,V^n) \geq \left(1 - e^{-n\Omega(\delta)}\right) H_{\Psi(\mathcal{C}_n,1)}(S^n|w^n(J),V^n) - 2e^{-\gamma_4 n}\log\left(\frac{|\mathcal{S}|^n|\mathcal{V}|^n}{e^{-\gamma_4 n}}\right) \tag{A76}$$

$$= \sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,1)}(S_i|w_i(J),V_i) - e^{-n\Omega(\delta)}\sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,1)}(S_i|w_i(J),V_i) - o(1) \tag{A77}$$

$$\geq \sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,1)}(S_i|w_i(J),V_i) - ne^{-n\Omega(\delta)}H_Q(S|V) - o(1) \tag{A78}$$

$$= \left[\sum_{i=1}^{n} H_{\Psi(\mathcal{C}_n,1)}(S_i|w_i(J),V_i)\right] - o(1) \tag{A79}$$

$$= nH_Q(S|W,V) - o(1). \tag{A80}$$

Finally, consider the case $H = 1$ and $Q_U \neq P_U$. We have for δ' small enough that

$$\mathbb{P}_{\tilde{P}(\mathcal{C}_n,1)}(M=0) = \mathbb{P}_{\tilde{P}(\mathcal{C}_n,1)}\left(U^n \notin \mathcal{T}^n_{[P_U]_{\delta'}}\right) \geq 1 - e^{-n(D(P_U||Q_U)-O(\delta'))} \xrightarrow{(n)} 1. \tag{A81}$$

Hence, for δ' small enough, we can write

$$H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|M,V^n) \geq H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|M,V^n,\Pi(U^n,\delta',P_U))$$

$$\geq \left(1 - e^{-n(D(P_U||Q_U)-O(\delta'))}\right) H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|M,V^n,\Pi(U^n,\delta',P_U)=1) \tag{A82}$$

$$= \left(1 - e^{-n(D(P_U||Q_U)-O(\delta'))}\right) H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|V^n,\Pi(U^n,\delta',P_U)=1) \tag{A83}$$

$$\geq \left(1 - e^{-n(D(P_U||Q_U)-O(\delta'))}\right) \left(H_{\tilde{P}(\mathcal{C}_n,1)}(S^n|V^n) - o(1)\right) \tag{A84}$$

$$= nH_Q(S|V) - ne^{-n(D(P_U||Q_U)-O(\delta'))}H_Q(S|V) - o(1) = nH_Q(S|V) - o(1). \tag{A85}$$

Here, (A82) follows from (A81); (A83) follows since $\Pi(U^n,\delta',P_U) = 1$ implies $M = 0$; (A84) follows from Lemma 3 and (15). Thus, since $\delta > 0$ is arbitrary, we have shown that for $\epsilon \in (0,1)$, $(R,\kappa,\Lambda_0,\Lambda_1) \in \mathcal{R}_e(\epsilon)$ if (18)–(21) holds.

On the other hand, average distortion of S^n at the detector can be lower bounded under $H = 0$ as follows:

$$\min_{g^{(r)}_{i,n}} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=0\right]$$

$$= \min_{\left\{\bar{\phi}_{i,n}(m,v^n,s^{i-1})\right\}_{i=1}^{n}} \mathbb{E}_{\tilde{P}(\mathcal{C}_n,0)}\left[\sum_{i=1}^{n} d\left(S_i,\bar{\phi}_i(m,v^n,s^{i-1})\right)\right] \tag{A86}$$

$$\geq \min_{\left\{\bar{\phi}_i(m,v^n,s^{i-1})\right\}_{i=1}^{n}} \mathbb{E}_{\Psi(\mathcal{C}_n,0)}\left[\sum_{i=1}^{n} d(S_i,\bar{\phi}_i(m,v^n,s^{i-1}))\right] - ne^{-n\gamma_4}D_m \tag{A87}$$

$$\geq \min_{\left\{\bar{\phi}_i(\cdot,\cdot)\right\}_{i=1}^{n}} \mathbb{E}_{\Psi(\mathcal{C}_n,0)}\left[\sum_{i=1}^{n} d(S_i,\bar{\phi}_i(w_i(J),V_i))\right] - ne^{-n\gamma_4}D_m \tag{A88}$$

$$\geq n \min_{\left\{\phi(\cdot,\cdot)\right\}} \mathbb{E}_P\left[d(S,\phi(W,V))\right] - n\left(e^{-n\gamma_4}+e^{-n\gamma_5}\right)D_m \tag{A89}$$

$$= n \min_{\left\{\phi(\cdot,\cdot)\right\}_{i=1}^{n}} \mathbb{E}_P\left[d(S,\phi(W,V))\right] - o(1). \tag{A90}$$

Here, (A86) follows from Lemma 2; (A87) follows from ([43], Property 2(b)) due to (A65) and boundedness of distortion measure; (A88) follows from the Markov chain in (A64); (A89) follows from (A67) and the fact that $\Psi^{(0)}_{S_iV_i|w_i(J)} = P^{(0)}_{SV|W}$, $i \in [n]$.

Next, consider the case $H = 1$ and $Q_U = P_U$. Then, similarly to above, we can write

$$\min_{g^{(r)}_{i,n}} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right]$$

$$= \min_{\left\{\bar{\phi}_i(m,v^n,s^{i-1})\right\}_{i=1}^{n}} \mathbb{E}_{\tilde{P}(\mathcal{C}_n,1)}\left[\sum_{i=1}^{n} d\left(S_i,\phi_i(M,V^n,S^{i-1})\right)\right]$$

$$\geq \min_{\left\{\bar{\phi}_i(m,v^n,s^{i-1})\right\}_{i=1}^{n}} \mathbb{E}_{\Psi(\mathcal{C}_n,1)}\left[\sum_{i=1}^{n} d(S_i,\phi_i(M,V^n,S^{i-1}))\right] - ne^{-n\gamma_4}D_m \tag{A91}$$

$$\geq \min_{\left\{\phi_i(\cdot,\cdot)\right\}_{i=1}^{n}} \mathbb{E}_{\Psi(\mathcal{C}_n,1)}\left[\sum_{i=1}^{n} d(S_i,\phi_i(w_i,V_i))\right] - ne^{-n\gamma_4}D_m \tag{A92}$$

$$\geq n \min_{\left\{\phi(\cdot,\cdot)\right\}_{i=1}^{n}} \mathbb{E}_Q\left[d(S,\phi(W,V))\right] - n(e^{-n\gamma_4}+e^{-n\gamma_5})D_m. \tag{A93}$$

$$= n \min_{\left\{\phi(\cdot,\cdot)\right\}_{i=1}^{n}} \mathbb{E}_Q\left[d(S,\phi(W,V))\right] - o(1). \tag{A94}$$

If $H = 1$ and $Q_U \neq P_U$, we have

$$\min_{g^{(r)}_{i,n}} \mathbb{E}\left[d\left(S^n,\hat{S}^n\right)|H=1\right]$$

$$\geq \mathbb{P}_{\tilde{P}(\mathcal{C}_n,1)}\left(M=0|H=1\right) \min_{\left\{\bar{\phi}_i(m,v^n,s^{i-1})\right\}_{i=1}^{n}} \sum_{i=1}^{n} \mathbb{E}_{\tilde{P}(\mathcal{C}_n,1)}\left[d\left(S_i,\phi_i(0,V^n,S^{i-1})\right)\right]$$

$$\geq \mathbb{P}_{\tilde{P}(\mathcal{C}_n,1)}\left(M=0|H=1\right)\left[\min_{\left\{\phi'_i(v)\right\}_{i=1}^{n}} \mathbb{E}_Q\left[\sum_{i=1}^{n} d(S_i,\phi'_i(V_i))\right] - D_m o(1)\right] \tag{A95}$$

$$= n \min_{\left\{\phi'(\cdot)\right\}} \mathbb{E}_Q\left[d(S,\phi'(V))\right] - o(1). \tag{A96}$$

Here, (A95) follows from (15) in Lemma 4 and (A96) follows from (A81). Thus, since $\delta > 0$ is arbitrary, we have shown that $(R,\kappa,\Delta_0,\Delta_1) \in \mathcal{R}_d(\epsilon)$, $\epsilon \in (0,1)$, provided that (18), (19), (24) and (25) are satisfied. This completes the proof of the theorem.

Appendix E. Proof of Lemma 5

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

$$P_U(u_i) = \sum_{w\in\mathcal{W}} P_W(w)P_{U|W}(u_i|w), i = 1,2,\ldots,|\mathcal{U}|-1, \tag{A97}$$

$$H_P(U|W,Z) = \sum_w P_W(w)g_1(P_{U|W},w), \tag{A98}$$

$$H_P(Y|W,Z) = \sum_w P_W(w)g_2(P_{U|W},w), \tag{A99}$$

$$H_P(S|W,Y,Z) = \sum_w P_W(w)g_3(P_{U|W},w), \tag{A100}$$

where

$$g_1(P_{U|W},w) = -\sum_{u,z} P_{U|W}(u|w)P_{Z|U}(z|u)\log\left(\frac{P_{U|W}(u|w)P_{Z|U}(z|u)}{\sum_u P_{U|W}(u|w)P_{Z|U}(z|u)}\right),$$

$$g_2(P_{U|W},w) = -\sum_{y,z,u} P_{U|W}(u|w)P_{YZ|U}(y,z|u)\log\left(\frac{\sum_u P_{U|W}(u|w)P_{YZ|U}(y,z|u)}{\sum_u P_{U|W}(u|w)P_{Z|U}(z|u)}\right),$$

$$g_3(P_{U|W},w) = -\sum_{s,y,z,u} P_{U|W}(u|w)P_{SYZ|U}(s,y,z|u)\log\left(\frac{\sum_u P_{U|W}(u|w)P_{SYZ|U}(s,y,z|u)}{\sum_u P_{U|W}(u|w)P_{YZ|U}(y,z|u)}\right).$$

Thus, by the Fenchel–Eggleston–Carathéodory's theorem [68], 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 (28)–(30). This completes the proof for the case of $\mathcal{R}_e$. Similarly, considering the $|\mathcal{U}|+1$ functions of $P_{W|U}$ given in (A97)–(A99) and

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

where

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

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

References

1. Appari, A.; Johnson, E. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterp. Manag.* **2010**, *6*, 279–314.
2. Gross, R.; Acquisti, A. Information revelation and privacy in online social networks. In Proceedings of the ACM workshop on Privacy in Electronic Society, Alexandria, VA, USA, 7 November 2005; pp. 71–80.
3. Miyazaki, A.; Fernandez, A. Consumer Perceptions of Privacy and Security Risks for Online Shopping. *J. Consum. Aff.* **2001**, *35*, 27–44.
4. Giaconi, G.; Gündüz, D.; Poor, H.V. Privacy-Aware Smart Metering: Progress and Challenges. *IEEE Signal Process. Mag.* **2018**, *35*, 59–78.

5. Ahlswede, R.; Csiszár, I. Hypothesis Testing with Communication Constraints. *IEEE Trans. Inf. Theory* **1986**, *32*, 533–542.
6. Han, T.S. Hypothesis Testing with Multiterminal Data Compression. *IEEE Trans. Inf. Theory* **1987**, *33*, 759–772.
7. Shimokawa, H.; Han, T.S.; Amari, S. Error Bound of Hypothesis Testing with Data Compression. In Proceedings of the IEEE International Symposium on Information Theory, Trondheim, Norway, 27 June–1 July 1994.
8. Shalaby, H.M.H.; Papamarcou, A. Multiterminal Detection with Zero-Rate Data Compression. *IEEE Trans. Inf. Theory* **1992**, *38*, 254–267.
9. Zhao, W.; Lai, L. Distributed Testing Against Independence with Multiple Terminals. In Proceedings of the 52nd Annual Allerton Conference, Monticello, IL, USA, 30 September–3 October 2014; pp. 1246–1251.
10. Katz, G.; Piantanida, P.; Debbah, M. Distributed Binary Detection with Lossy Data Compression. *IEEE Trans. Inf. Theory* **2017**, *63*, 5207–5227.
11. Rahman, M.S.; Wagner, A.B. On the Optimality of Binning for Distributed Hypothesis Testing. *IEEE Trans. Inf. Theory* **2012**, *58*, 6282–6303.
12. Sreekumar, S.; Gündüz, D. Distributed Hypothesis Testing Over Noisy Channels. In Proceedings of the IEEE International Symposium on Information Theory, Aachen, Germany, 25–30 June 2017; pp. 983–987.
13. Sreekumar, S.; Gündüz, D. Distributed Hypothesis Testing Over Discrete Memoryless Channels. *IEEE Trans. Inf. Theory* **2020**, *66*, 2044–2066.
14. Salehkalaibar, S.; Wigger, M.; Timo, R. On Hypothesis Testing Against Conditional Independence with Multiple Decision Centers. *IEEE Trans. Commun.* **2018**, *66*, 2409–2420.
15. Salehkalaibar, S.; Wigger, M. Distributed Hypothesis Testing based on Unequal-Error Protection Codes. *arXiv* **2018**, arXiv:1806.05533.
16. Han, T.S.; Kobayashi, K. Exponential-Type Error Probabilities for Multiterminal Hypothesis Testing. *IEEE Trans. Inf. Theory* **1989**, *35*, 2–14.
17. Haim, E.; Kochman, Y. On Binary Distributed Hypothesis Testing. *arXiv* **2018**, arXiv:1801.00310.
18. Weinberger, N.; Kochman, Y. On the Reliability Function of Distributed Hypothesis Testing Under Optimal Detection. *IEEE Trans. Inf. Theory* **2019**, *65*, 4940–4965.
19. Bayardo, R.; Agrawal, R. Data privacy through optimal k-anonymization. In Proceedings of the International Conference on Data Engineering, Tokyo, Japan, 5–8 April 2005; pp. 217–228.
20. Agrawal, R.; Srikant, R. Privacy-preserving data mining. In Proceedings of the ACM SIGMOD International Conference on Management of Data, Dallas, USA, 18–19 May 2000; pp. 439–450.
21. Bertino, E. Big Data-Security and Privacy. In Proceedings of the IEEE International Congress on BigData, New York, NY, USA, 27 June–2 July 2015; pp. 425–439.
22. Gertner, Y.; Ishai, Y.; Kushilevitz, E.; Malkin, T. Protecting Data Privacy in Private Information Retrieval Schemes. *J. Comput. Syst. Sci.* **2000**, *60*, 592–629.
23. Hay, M.; Miklau, G.; Jensen, D.; Towsley, D.; Weis, P. Resisting structural re-identification in anonymized social networks. *J. Proc. VLDB Endow.* **2008**, *1*, 102–114.
24. Narayanan, A.; Shmatikov, V. De-anonymizing Social Networks. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 17–20 May 2009.
25. Liao, J.; Sankar, L.; Tan, V.; Calmon, F. Hypothesis Testing Under Mutual Information Privacy Constraints in the High Privacy Regime. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1058–1071.
26. Liao, J.; Sankar, L.; Calmon, F.; Tan, V. Hypothesis testing under maximal leakage privacy constraints. In Proceedings of the IEEE International Symposium on Information Theory, Aachen, Germany, 25–30 June 2017.
27. Gilani, A.; Amor, S.B.; Salehkalaibar, S.; Tan, V. Distributed Hypothesis Testing with Privacy Constraints. *Entropy* **2019**, *21*, 1–27.
28. Gündüz, D.; Erkip, E.; Poor, H.V. Secure lossless compression with side information. In Proceedings of the IEEE Information Theory Workshop, Porto, Portugal, 5–9 May 2008; pp. 169–173.
29. Gündüz, D.; Erkip, E.; Poor, H.V. Lossless compression with security constraints. In Proceedings of the IEEE International Symposium on Information Theory, Toronto, ON, Canada, 6–11 July 2008; pp. 111–115.

30. Mhanna, M.; Piantanida, P. On secure distributed hypothesis testing. In Proceedings of the IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015; pp. 1605–1609.
31. Sweeney, L. K-anonymity: A model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl. Based Syst.* **2002**, *10*, 557–570.
32. Dwork, C.; McSherry, F.; Nissim, K.; Smith, A. Calibrating Noise to Sensitivity in Private Data Analysis. In *Theory of Cryptography*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 265–284.
33. Calmon, F.; Fawaz, N. Privacy Against Statistical Inference. In Proceedings of the 50th Annual Allerton Conference, IL, USA, 1–5 October 2012; pp. 1401–1408.
34. Makhdoumi, A.; Salamatian, S.; Fawaz, N.; Medard, M. From the information bottleneck to the privacy funnel. In Proceedings of the IEEE Information Theory Workshop, Hobart, Australia, 2–5 November 2014; pp. 501–505.
35. Calmon, F.; Makhdoumi, A.; Medard, M. Fundamental limits of perfect privacy. In Proceedings of the IEEE International Symposium on Information Theory, Hong Kong, China, 14–19 June 2015; pp. 1796–1800.
36. Issa, I.; Kamath, S.; Wagner, A.B. An Operational Measure of Information Leakage. In Proceedings of the Annual Conference on Information Science and Systems, Princeton, NJ, USA, 16–18 March 2016; pp. 1–6.
37. Rassouli, B.; Gündüz, D. Optimal Utility-Privacy Trade-off with Total Variation Distance as a Privacy Measure. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 594–603.
38. Wagner, I.; Eckhoff, D. Technical Privacy Metrics: A Systematic Survey. *arXiv* **2015**, arXiv:1512.00327v1.
39. Goldwasser, S.; Micali, S. Probabilistic encryption. *J. Comput. Syst. Sci.* **1984**, *28*, 270–299.
40. Bellare, M.; Tessaro, S.; Vardy, A. Semantic Security for the Wiretap Channel. In Proceedings of the Advances in Cryptology-CRYPTO 2012, Heidelberg, Germany, 19–23 August 2012; pp. 294–311.
41. Yamamoto, H. A Rate-Distortion Problem for a Communication System with a Secondary Decoder to be Hindered. *IEEE Trans. Inf. Theory* **1988**, *34*, 835–842.
42. Tandon, R.; Sankar, L.; Poor, H.V. Discriminatory Lossy Source Coding: Side Information Privacy. *IEEE Trans. Inf. Theory* **2013**, *59*, 5665–5677.
43. Schieler, C.; Cuff, P. Rate-Distortion Theory for Secrecy Systems. *IEEE Trans. Inf. Theory* **2014**, *60*, 7584–7605.
44. Agarwal, G.K. On Information Theoretic and Distortion-based Security. Ph.D. Thesis, University of California, Los Angeles, 2019. Available online: https://escholarship.org/uc/item/7qs7z91g (accessed on 3 January 2020).
45. Li, Z.; Oechtering, T.; Gündüz, D. Privacy against a hypothesis testing adversary. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1567–1581.
46. Cuff, P.; Yu, L. Differential privacy as a mutual information constraint. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 24–28 October 2016; pp. 43–54.
47. Goldfeld, Z.; Cuff, P.; Permuter, H.H. Semantic-Security Capacity for Wiretap Channels of Type II. *IEEE Trans. Inf. Theory* **2016**, *62*, 3863–3879.
48. Sreekumar, S.; Bunin, A.; Goldfeld, Z.; Permuter, H.H.; Shamai, S. The Secrecy Capacity of Cost-Constrained Wiretap Channels. *arXiv* **2020**, arXiv:2004.04330.
49. Kasiviswanathan, S.P.; Lee, H.K.; Nissim, K.; Raskhodnikova, S.; Smith, A. What can we learn privately? *SIAM J. Comput.* **2011**, *40*, 793–826.
50. Duchi, J.C.; Jordan, M.I.; Wainwright, M.J. Local Privacy and Statistical Minimax Rates. 2013 IEEE 54th Annual Symposium on Foundations of Computer Science, 26–29 October 2013; pp. 429–438.
51. Duchi, J.C.; Jordan, M.I.; Wainwright, M.J. Privacy Aware Learning. *J. ACM* **2014**, *61*, 1–57.
52. Wang, Y.; Lee, J.; Kifer, D. Differentially Private Hypothesis Testing, Revisited. *arXiv* **2015**, arXiv:1511.03376.
53. Gaboardi, M.; Lim, H.; Rogers, R.; Vadhan, S. Differentially Private Chi-Squared Hypothesis Testing: Goodness of Fit and Independence Testing. In Proceedings of the 33rd International Conference on Machine Learning, New York City, NY, USA, 19–24 June 2016; Volume 48, pp. 2111–2120.
54. Rogers, R.M.; Roth, A.; Smith, A.D.; Thakkar, O. Max-Information, Differential Privacy, and Post-Selection Hypothesis Testing. *arXiv* **2016** arXiv:1604.03924.
55. Cai, B.; Daskalakis, C.; Kamath, G. Priv'IT: Private and Sample Efficient Identity Testing. In Proceedings of the 34th International Conference on Machine Learning, Sydney, Australia, 6–11 August 2017; Volume 70, pp. 635–644.

56. Sheffet, O. Locally Private Hypothesis Testing. In Proceedings of the 35th International Conference on Machine Learning, Stockholm, Sweden, 10–15 July 2018; Volume 80, pp. 4605–4614.
57. Acharya, J.; Sun, Z.; Zhang, H. Differentially Private Testing of Identity and Closeness of Discrete Distributions. In *Advances in Neural Information Processing Systems 31*, Curran Associates Inc.: Red Hook, NY, USA, 2018; pp. 6878–6891.
58. Canonne, C.L.; Kamath, G.; McMillan, A.; Smith, A.; Ullman, J. The Structure of Optimal Private Tests for Simple Hypotheses. In Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, Phoenix, Arizona, 23–26 June 2019; pp. 310–321.
59. Aliakbarpour, M.; Diakonikolas, I.; Kane, D.; Rubinfeld, R. Private Testing of Distributions via Sample Permutations. In *Advances in Neural Information Processing Systems 32*; Curran Associates Inc.: Red Hook, NY, USA, 2019; pp. 10878–10889.
60. Csiszár, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*; Cambridge University Press: Cambridge, UK, 2011.
61. Wang, Y.; Basciftci, Y.O.; Ishwar, P. Privacy-Utility Tradeoffs under Constrained Data Release Mechanisms. *arXiv* **2017**, arXiv:1710.09295.
62. Cuff, P. Distributed Channel Synthesis. *IEEE Trans. Inf. Theory* **2013**, *59*, 7071–7096.
63. Song, E.C.; Cuff, P.; Poor, H.V. The Likelihood Encoder for Lossy Compression. *IEEE Trans. Inf. Theory* **2016**, *62*, 1836–1849.
64. Wyner, A.D. The Common Information of Two Dependent Random Variables. *IEEE Trans. Inf. Theory* **1975**, *21*, 163–179. rXiv
65. Han, T.S.; Verdú, S. Approximation Theory of Output Statistics. *IEEE Trans. Inf. Theory* **1993**, *39*, 752–772.
66. Sreekumar, S.; Gündüz, D.; Cohen, A. Distributed Hypothesis Testing Under Privacy Constraints. In Proceedings of the IEEE Information Theory Workshop (ITW), Guangzhou, China, 25–29 November 2018; pp. 1–5.
67. Tishby, N.; Pereira, F.; Bialek, W. The Information Bottleneck Method. *arXiv* **2000**, arXiv:physics/0004057.
68. Gamal, A.E.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011.
69. Polyanskiy, Y. Channel Coding: Non-Asymptotic Fundamental Limits. Ph.D. Thesis, Princeton University, Princeton, NJ, USA, 2010.
70. Yang, W.; Caire, G.; Durisi, G.; Polyanskiy, Y. Optimum Power Control at Finite Blocklength. *IEEE Trans. Inf. Theory* **2015**, *61*, 4598–4615.
71. Villard, J.; Piantanida, P. Secure Multiterminal Source Coding With Side Information at the Eavesdropper. *IEEE Trans. Inf. Theory* **2013**, *59*, 3668–3692.
72. Gallager, R.G. A simple derivation of the coding theorem and some applications. *IEEE Trans. Inf. Theory* **1965**, *11*, 3–18.