entropy

MDPI

Article

Distributed Hypothesis Testing with Privacy Constraints

Atefeh Gilani [1], Selma Belhadj Amor [2], Sadaf Salehkalaibar [1,*] and Vincent Y. F. Tan [2]

[1] Department of Electrical and Computer Engineering, College of Engineering, University of Tehran, Tehran 14171614418, Iran; atefehgilani@ut.ac.ir

[2] Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore; selma.belhadjamor@gmail.com (S.B.A.); vtan@nus.edu.sg (V.Y.F.T.)

* Correspondence: s.saleh@ut.ac.ir

Received: 6 February 2019; Accepted: 20 March 2019; Published: 7 May 2019

Abstract: We revisit the distributed hypothesis testing (or hypothesis testing with communication constraints) problem from the viewpoint of privacy. Instead of observing the raw data directly, the transmitter observes a sanitized or randomized version of it. We impose an upper bound on the mutual information between the raw and randomized data. Under this scenario, the receiver, which is also provided with side information, is required to make a decision on whether the null or alternative hypothesis is in effect. We first provide a general lower bound on the type-II exponent for an arbitrary pair of hypotheses. Next, we show that if the distribution under the alternative hypothesis is the product of the marginals of the distribution under the null (i.e., testing against independence), then the exponent is known exactly. Moreover, we show that the strong converse property holds. Using ideas from Euclidean information theory, we also provide an approximate expression for the exponent when the communication rate is low and the privacy level is high. Finally, we illustrate our results with a binary and a Gaussian example.

Keywords: hypothesis testing; privacy; mutual information; testing against independence; zero-rate communication

1. Introduction

In the distributed hypothesis testing (or hypothesis testing with communication constraints) problem, some observations from the environment are collected by the sensors in a network. They describe these observations over the network which are finally received by the decision center. The goal is to guess the joint distribution governing the observations at terminals. In particular, there are two possible hypotheses $\mathcal{H} = 0$ or $\mathcal{H} = 1$, where the joint distribution of the observations is specified under each of them. The performance of this system is characterized by two criteria: the type-I and the type-II error probabilities. The probability of deciding on $\mathcal{H} = 1$ (respectively $\mathcal{H} = 0$) when the original hypothesis is $\mathcal{H} = 0$ (respectively $\mathcal{H} = 1$) is referred to as the type-I error (type-II error) probability. There are several approaches for defining the performance of a hypothesis test. First, we can maximize the exponent (exponential rate of decay) of the Bayesian error probability. Second, we can impose that the type-II error probability decays exponentially fast and we can then maximize the exponent of the type-I error probability; this is known as the Hoeffding regime. The approach in this work is the Chernoff-Stein regime in which we upper bound the type-II error probability by a non-vanishing constant and we maximize the exponent of the type-II error probability.

A special case of interest is testing against independence where the joint distribution under $\mathcal{H} = 1$ is the product of the marginals under $\mathcal{H} = 0$. The optimal exponent of type-II error probability for testing against independence is determined by Ahlswede and Csiszár in [1]. Several extensions of

this basic problem are studied for a multi-observer setup [2–6], a multi-decision center setup [7,8] and a setup with security constraints [9]. The main idea of the achievable scheme in these works is typicality testing [10,11]. The sensor finds a jointly typical codeword with its observation and sends the corresponding bin index to the decision center. The final decision is declared based on typicality check of the received codeword with the observation at the center. We note that the coding scheme employed here is reminiscent of those used for source coding with side information [12] and for different variants of the information bottleneck problem [13–16].

1.1. Injecting Privacy Considerations into Our System

We revisit the distributed hypothesis testing problem from a privacy perspective. In many applications such as healthcare systems, there is a need to randomize the data before publishing it. For example, hospitals often have large amounts of medical records of their patients. These records are useful for performing various statistical inference tasks, such as learning about causes of a certain ailment. However, due to privacy considerations of the patients, the data cannot be published as is. The data needs to be sanitized, quantized, perturbed and then be fed to a management center before statistical inference, such as hypothesis testing, is being done.

In the proposed setup, we use a privacy mechanism to sanitize the observation at the terminal before it is compressed; see Figure 1. The compression is performed at a separate terminal called *transmitter*, which communicates the randomized data over a noiseless link of rate R to a receiver. The hypothesis testing is performed using the received data (the compression index and additional side information) to determine the correct hypothesis governing the original observations. The privacy criterion is defined by the mutual information [17–20] of the published and original data.

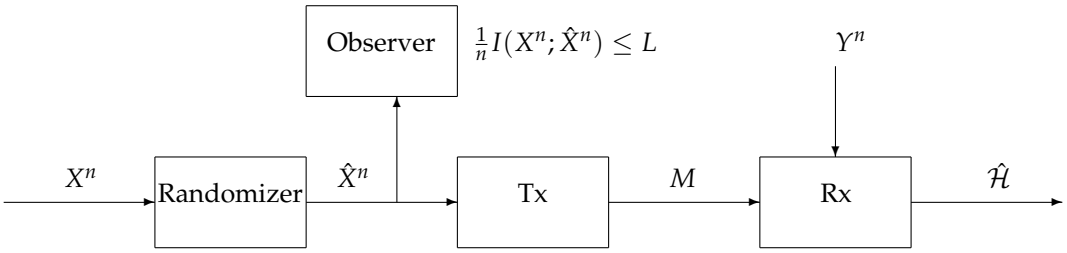

Figure 1. Hypothesis testing with communication and privacy constraints.

There is a long history of research to provide appropriate metrics to measure privacy. To quantify the information leakage an observation $\hat{X}$ can induce on a latent variable X, Shannon's mutual information $I(X;\hat{X})$ is considered in [17–20]. Smith [18] proposed to use Arimoto's mutual information of order ∞, $I_\infty(X;\hat{X})$. Barthe and Köpf [21–23] proposed the maximal information leakage $\max_{P_X} I_\infty(X;\hat{X})$. We refer the reader to [24] for a survey on the existing information leakage measures. A different line of works, in statistics, computer science, and other related fields, concerns *differential privacy*, initially proposed in [25]. Furthermore, a generalized notion—(ϵ,δ)-differential privacy [26]—provides a unified mathematical framework for data privacy. The reader is referred to the survey by Dwork [27] and the statistical framework studied by Wasserman and Zhou [28] and the references therein.

The privacy mechanism can be either memoryless or non-memoryless. In the former, the distribution of the randomized data at each time instant depends on the original sequence at the same time and not on the previous history of the data.

1.2. Description of Our System Model

We propose a coding scheme for the proposed setup. The idea is that the sensor, upon observing the source sequence, performs a typicality test and obtains its belief of the hypothesis. If the belief is $\mathcal{H} = 0$, it publishes the randomized data based on a specific memoryless mechanism. However,

if its belief is $\mathcal{H} = 1$, it sends an all-zero sequence to let the transmitter know about its decision. The transmitter communicates the received data, which is a sanitized version of the original data or an all-zero sequence, over the noiseless link to the receiver. In this scheme, the whole privacy mechanism is non-memoryless since the typicality check of the source sequence which uses the history of the observation, determines the published data. It is shown that the achievable error exponent recovers previous results on hypothesis testing with zero and positive communication rates in [10]. Our work is related to a recent work [29] where a general hypothesis testing setup is considered from a privacy perspective. However, in [29], the problem at hand is different from ours. The authors consider equivocation and average distortion as possible measures of privacy whereas we constrain the mutual information between the original and released (published) data.

A difference of the proposed scheme with some previous works is highlighted as follows. The privacy mechanism even if it is memoryless, cannot be viewed as a noiseless link of a rate equivalent to the privacy criterion. Particularly, the proposed model is different from cascade hypothesis testing problem of [8] or similar works [3,4] which consider consecutive noiseless links for data compression and distributed hypothesis testing. The difference comes from the fact that in these works, a codeword is chosen jointly typical with the observed sequence at the terminal and its corresponding index is sent over the noiseless link. However, in our model, the randomized sequence is not necessarily jointly typical with the original sequence. Thus, there is a need for an achievable scheme which lets the transmitter know whether the original data is typical or not.

The problem of hypothesis testing against independence with a memoryless privacy mechanism is also considered. A coding scheme is proposed where the sensor outputs the randomized data based on the memoryless privacy mechanism. The optimality of the achievable type-II error exponent is shown by providing a strong converse. Specializing the optimal error exponent to a binary example shows that an increase in the privacy criterion (a less stringent privacy mechanism) results in a larger type-II error exponent. Thus, there exists a trade-off between privacy and hypothesis testing criteria. The optimal type-II error exponent is further studied for the case of restricted privacy mechanism and zero-rate communication. The Euclidean approach of [30–33] is used to approximate the error exponent for this regime. The result confirms the trade-off between the privacy criterion and type-II error exponent. Finally, a Gaussian setup is proposed and its optimal error exponent is established.

1.3. Main Contributions

The contributions of the paper are listed in the following:

- An achievable type-II error exponent is proposed using a non-memoryless privacy mechanism (Theorem 1 in Section 3);
- The optimal error exponent of testing against independence with a memoryless privacy mechanism is determined. In addition, a strong converse is also proved (Theorem 2 in Section 4.1);
- A binary example is proposed to show the trade-off between the privacy and error exponent (Section 4.3);
- An Euclidean approximation [30] of the error exponent is provided (Section 4.4);
- A Gaussian setup is proposed and its optimal error exponent is derived (Proposition 2 in Section 4.5).

1.4. Notation

The notation mostly follows [34]. Random variables are denoted by capital letters, e.g., X, Y, and their realizations by lower case letters, e.g., x, y. The alphabet of the random variable X is denoted as $\mathcal{X}$. Sequences of random variables and their realizations are denoted by $(X_i, \ldots, X_j)$ and $(x_i, \ldots, x_j)$ and are abbreviated as X_i^j and x_i^j. We use the alternative notation X^j when $i = 1$. Vectors and matrices are denoted by boldface letters, e.g., $\mathbf{k}$, $\mathbf{W}$. The ℓ_2-norm of $\mathbf{k}$ is denoted as $\|\mathbf{k}\|$. The notation $\mathbf{k}^T$ denotes the transpose of $\mathbf{k}$.

The probability mass function (pmf) of a discrete random variable X is denoted as P_X, the conditional pmf of X given Y is denoted as $P_{X|Y}$. The notation $D(P_X\|Q_X)$ denotes the Kullback-Leibler (KL) divergence between two pmfs P_X and Q_X. The total variation distance between two pmfs P_X and Q_X is denoted by $|P_X - Q_X| = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)|$. We use $\mathrm{tp}(x^n, y^n)$ to denote the joint type of (x^n, y^n).

For a given P_{XY} and a positive number μ, we denote by $\mathcal{T}_\mu^n(P_{XY})$, the set of jointly μ-typical sequences [34], i.e., the set of all (x^n, y^n) whose joint type is within μ of P_{XY} (in the sense of total-variation distance). The notation $\mathcal{T}^n(P_X)$ denotes for the type class of the type P_X.

The notation $h_\mathrm{b}(\cdot)$ denotes the binary entropy function, $h_\mathrm{b}^{-1}(\cdot)$ its inverse over $\left[0, \frac{1}{2}\right]$, and $a \star b \triangleq a(1-b) + (1-a)b$ for $0 \le a, b \le 1$. The differential entropy of a continuous random variable X is $h(X)$. All logarithms $\log(\cdot)$ are taken with respect to base 2.

1.5. Organization

The remainder of the paper is organized as follows. Section 2 describes a mathematical setup for our proposed problem. Section 3 discusses hypothesis testing with general distributions. The results for hypothesis testing against independence with a memoryless privacy mechanism are provided in Section 4. The paper is concluded in Section 5.

2. System Model

Let $\mathcal{X}$, $\mathcal{Y}$, and $\hat{\mathcal{X}}$ be arbitrary finite alphabets and let n be a positive integer. Consider the hypothesis testing problem with communication and privacy constraints depicted in Figure 1. The first terminal in the system, the *Randomizer*, receives the sequence $X^n = (X_1, \ldots, X_n) \in \mathcal{X}^n$ and outputs the sequence $\hat{X}^n = (\hat{X}_1, \ldots, \hat{X}_n) \in \hat{\mathcal{X}}^n$, which is a noisy version of X^n under a *privacy mechanism* determined by the conditional probability distribution $P_{\hat{X}^n|X^n}$; the second terminal, the *Transmitter*, receives the sequence $\hat{X}^n$; the third terminal, the *Receiver*, observes the side-information sequence $Y^n = (Y_1, \ldots, Y_n) \in \mathcal{Y}^n$. Under the null hypothesis

$$\mathcal{H} = 0: \quad (X^n, Y^n) \sim \text{i.i.d. } P_{XY}, \tag{1}$$

whereas under the alternative hypothesis

$$\mathcal{H} = 1: \quad (X^n, Y^n) \sim \text{i.i.d. } Q_{XY}, \tag{2}$$

for two given pmfs P_{XY} and Q_{XY}.

The privacy mechanism is described by the conditional pmf $P_{\hat{X}^n|X^n}$ which maps each sequence $X^n \in \mathcal{X}^n$ to a sequence $\hat{X}^n \in \hat{\mathcal{X}}^n$. For any $(\hat{x}^n, x^n, y^n) \in \hat{\mathcal{X}}^n \times \mathcal{X}^n \times \mathcal{Y}^n$, the joint distributions considering the privacy mechanism are given by

$$P^n_{\hat{X}XY}(\hat{x}^n, x^n, y^n) \triangleq P_{\hat{X}^n|X^n}(\hat{x}^n|x^n) \cdot \prod_{i=1}^n P_{XY}(x_i, y_i), \tag{3}$$

$$Q^n_{\hat{X}XY}(\hat{x}^n, x^n, y^n) \triangleq P_{\hat{X}^n|X^n}(\hat{x}^n|x^n) \cdot \prod_{i=1}^n Q_{XY}(x_i, y_i). \tag{4}$$

A *memoryless/local* privacy mechanism is defined by a conditional pmf $P_{\hat{X}|X}$ which stochastically and independently maps each entry $X_i \in \mathcal{X}$ of X^n to a released $\hat{X}_i \in \hat{\mathcal{X}}$ to construct $\hat{X}^n$. Consequently, for the memoryless privacy mechanism, the conditional pmf $P_{\hat{X}^n|X^n}(\hat{x}^n|x^n)$ factorizes as follows:

$$rCl \qquad P_{\hat{X}^n|X^n}(\hat{x}^n|x^n) = \prod_{i=1}^n P_{\hat{X}|X}(\hat{x}_i|x_i) = P^n_{\hat{X}|X}(\hat{x}^n|x^n), \qquad \forall (\hat{x}^n, x^n) \in \hat{\mathcal{X}}^n \times \mathcal{X}^n. \tag{5}$$

There is a noise-free bit pipe of rate R from the transmitter to the receiver. Upon observing $\hat{X}^n$, the transmitter computes the message $M = \phi^{(n)}(\hat{X}^n)$ using a possibly stochastic encoding function $\phi^{(n)} : \hat{\mathcal{X}}^n \to \{0, \ldots, \lfloor 2^{nR} \rfloor\}$ and sends it over the bit pipe to the receiver.

The goal of the receiver is to produce a guess of $\mathcal{H}$ using a decoding function $g^{(n)} : \mathcal{Y}^n \times \{0, ..., \lfloor 2^{nR} \rfloor\} \to \{0, 1\}$ based on the observation Y^n and the received message M. Thus the estimate of the hypothesis is $\hat{\mathcal{H}} = g^{(n)}(Y^n, M)$.

This induces a partition of the sample space $\hat{\mathcal{X}}^n \times \mathcal{X}^n \times \mathcal{Y}^n$ into an acceptance region $\mathcal{A}_n$ defined as follows:

$$\mathcal{A}_n \triangleq \left\{ (\hat{x}^n, x^n, y^n) \colon g^{(n)}(y^n, \phi^{(n)}(\hat{x}^n)) = 0 \right\}, \tag{6}$$

and a rejection region denoted by $\mathcal{A}_n^c$.

Definition 1. *For any $\epsilon \in [0, 1)$ and for a given rate-privacy pair $(R, L) \in \mathbb{R}_+^2$, we say that a type-II exponent $\theta \in \mathbb{R}_+$ is (ϵ, R, L)-achievable if there exists a sequence of functions and conditional pmfs $(\phi^{(n)}, g^{(n)}, P_{\hat{X}^n|X^n})$, such that the corresponding sequences of type-I and type-II error probabilities at the receiver are defined as*

$$\alpha_n \triangleq P^n_{\hat{X}XY}(\mathcal{A}_n^c) \quad \textit{and} \quad \beta_n \triangleq Q^n_{\hat{X}XY}(\mathcal{A}_n), \tag{7}$$

respectively, and they satisfy

$$\limsup_{n\to\infty} \ \alpha_n \leq \epsilon \quad \textit{and} \quad \liminf_{n\to\infty} \ \frac{1}{n} \log \frac{1}{\beta_n} \geq \theta. \tag{8}$$

Furthermore, the privacy measure

$$T_n \triangleq \frac{1}{n} I(X^n; \hat{X}^n), \tag{9}$$

satisfies

$$\limsup_{n\to\infty} \ T_n \leq L. \tag{10}$$

The optimal exponent $\theta^*_\epsilon(R, L)$ is the supremum of all (ϵ, R, L)-achievable $\theta \in \mathbb{R}_+$.

3. General Hypothesis Testing

3.1. Achievable Error Exponent

The following presents an achievable error exponent for the proposed setup.

Theorem 1. *For a given $\epsilon \in [0, 1)$ and a rate-privacy pair $(R, L) \in \mathbb{R}_+^2$, the optimal type-II error exponent $\theta^*_\epsilon(R, L)$ for the multiterminal hypothesis testing setup under the privacy constraint L and the rate constraint R satisfies*

$$rCl\theta^*_\epsilon(R, L) \geq \max_{\substack{P_{U|\hat{X}}, P_{\hat{X}|X}: \\ R \geq I(U;\hat{X}) \\ L \geq I(X;\hat{X})}} \ \min_{\tilde{P}_{U\hat{X}XY} \in \mathcal{P}_{U\hat{X}XY}} D(\tilde{P}_{U\hat{X}XY} \| P_{U|\hat{X}} P_{\hat{X}|X} Q_{XY}), \tag{11}$$

where the set $\mathcal{P}_{U\hat{X}XY}$ is defined as

$$\mathcal{P}_{U\hat{X}XY} \triangleq \left\{ \tilde{P}_{U\hat{X}XY} \ \middle| \ \begin{array}{l} \tilde{P}_X = P_X, \\ \tilde{P}_{UY} = P_{UY}, \\ \tilde{P}_{U\hat{X}} = P_{U\hat{X}} \end{array} \right\}. \tag{12}$$

Given $P_{U|\hat{X}}$ and $P_{\hat{X}|X}$, the mutual informations in (11) are calculated according to the following joint distribution:

$$P_{U\hat{X}|X} \triangleq P_{U|\hat{X}} \cdot P_{\hat{X}|X}. \tag{13}$$

Proof. The coding scheme is given in the following section. For the analysis, see Appendix A. □

3.2. Coding Scheme

In this section, we propose a coding scheme for Theorem 1, under fixed rate and privacy constraints $(R, L) \in \mathbb{R}_+^2$. Fix the joint distribution $P_{U\hat{X}XY}$ as in (13). Let $P_U(u)$ be the marginal distribution of $U \in \mathcal{U}$ defined as

$$P_U(u) \triangleq \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{U|\hat{X}}(u|\hat{x}) \sum_{x\in\mathcal{X}} P_{\hat{X}X}(\hat{x}, x). \tag{14}$$

Fix positive $\mu > 0$ and $\zeta > 0$, an arbitrary blocklength n and two conditional pmfs $P_{\hat{X}|X}$ and $P_{U|\hat{X}}$ over finite auxiliary alphabets $\hat{\mathcal{X}}$ and $\mathcal{U}$. Fix also the rate and privacy leakage level as

$$R = I(U; \hat{X}) + \mu, \quad \text{and} \quad L = I(\hat{X}; X) + \zeta. \tag{15}$$

Codebook Generation: Randomly and independently generate a codebook

$$\mathcal{C}_U \triangleq \left\{ U^n(m) : m \in \{0, \ldots, \lfloor 2^{nR} \rfloor\} \right\}, \tag{16}$$

by drawing $U^n(m)$ in an i.i.d. manner according to P_U. The codebook is revealed to all terminals.

Randomizer: Upon observing x^n, it checks whether $x^n \in \mathcal{T}^n_{\mu/4}(P_X)$. If successful, it outputs the sequence $\hat{x}^n$ where its i-th component $\hat{x}_i$ is generated based on x_i, according to $P_{\hat{X}|X}(\hat{x}_i|x_i)$. If the typicality check is not successful, the randomizer then outputs 0^n which is an all-zero sequence of length n, where $\hat{x}^n = 0^n$.

Transmitter: Upon observing $\hat{x}^n$, if $\hat{x}^n \neq 0^n$, the transmitter finds an index m such that $\left(u^n(m), \hat{x}^n\right) \in \mathcal{T}^n_{\mu/2}(P_{U\hat{X}})$. If successful, it sends the index m over the noiseless link to the receiver. Otherwise, if the typicality check is not successful or $\hat{x}^n = 0^n$, it sends $m = 0$.

Receiver: Upon observing y^n and receiving the index m, if $m = 0$, the receiver declares $\hat{\mathcal{H}} = 1$. If $m \neq 0$, it checks whether $\left(u^n(m), y^n\right) \in \mathcal{T}^n_\mu(P_{UY})$. If the test is successful, the receiver declares $\hat{\mathcal{H}} = 0$; otherwise, it sets $\hat{\mathcal{H}} = 1$.

Remark 1. *In the above scheme, the sequence $\hat{X}^n$ is chosen to be an n-length zero-sequence when the randomizer finds that X^n is not typical according to P_X. Thus, the privacy mechanism is not memoryless and the sequence $\hat{X}^n$ is not identically and independently distributed (i.i.d.). A detailed analysis in Appendix A shows that the privacy criterion is not larger than L as the blocklength $n \to \infty$.*

3.3. Discussion

In the following, we discuss some special cases. First, suppose that $R = 0$. The following corollary shows that Theorem 1 recovers Han's result [1] for distributed hypothesis testing with zero-rate communication.

Corollary 1 (Theorem 5 in [10]). *Suppose that $Q_{XY} > 0$. For all $\epsilon \in [0,1)$, the optimal error exponent of the zero-rate communication for any privacy mechanism (including non-memoryless mechanisms) is given by the following:*

$$\theta_\epsilon^*(0,L) = \min_{\substack{\tilde{P}_{XY}: \\ \tilde{P}_X = P_X \\ \tilde{P}_Y = P_Y}} D(\tilde{P}_{XY} \| Q_{XY}). \tag{17}$$

Proof. The proof of achievability follows by Theorem 1, in which $\hat{X}$ is arbitrary and the auxiliary $U = \emptyset$ due to the zero-rate constraint. The proof of the strong converse follows along the same lines as [35]. □

Remark 2. *Consider the case of $R > 0$ and $L = 0$ where $\hat{X}$ is independent of X. Using Theorem 1, the optimal error exponent is lower bounded as follows:*

$$\theta_\epsilon^*(R,0) \geq \min_{\substack{\tilde{P}_{XY}: \\ \tilde{P}_X = P_X \\ \tilde{P}_Y = P_Y}} D(\tilde{P}_{XY} \| Q_{XY}). \tag{18}$$

However, there is no known converse result in this case where the communication rate is positive. Comparing this special case with the one in Corollary 1 shows that the proposed model does not, in general, admit symmetry between the rate and privacy constraints. However, we will see from some specific examples in the following that the roles of R and L are symmetric.

Now, suppose that L is so large such that $L > H(X)$. The following corollary shows that Theorem 1 recovers Han's result in [10] for distributed hypothesis testing over a rate-R communication link.

Corollary 2 (Theorem 2 in [10]). *Assuming $L > H(X)$, the optimal error exponent is lower bounded as the following:*

$$\theta_\epsilon^*(R,L) \geq \max_{\substack{P_{U|X}: \\ R \geq I(U;X)}} \min_{\substack{\tilde{P}_{UXY}: \\ \tilde{P}_{UX} = P_{UX} \\ \tilde{P}_{UY} = P_{UY}}} D(\tilde{P}_{UXY} \| P_{U|X} Q_{XY}). \tag{19}$$

Proof. The proof follows from Theorem 1 by specializing to $\hat{X} = X$. □

The above two special cases reveal a trade-off between the privacy criterion and the achievable error exponent when the communication rate is positive, i.e., $R > 0$. An increase in L results in a larger achievable error exponent. This observation is further illustrated by an example in Section 4.3 to follow.

4. Hypothesis Testing against Independence with a Memoryless Privacy Mechanism

In this section, we consider testing against independence where the joint pmf under $\mathcal{H} = 1$ factorizes as follows:

$$Q_{XY} = P_X \cdot P_Y. \tag{20}$$

The privacy mechanism is assumed to be memoryless here.

4.1. Optimal Error Exponent

The following theorem, which includes a strong converse, states the optimal error exponent for this special case.

Theorem 2. *For any $(R, L) \in \mathbb{R}_+^2$, define*

$$\theta_\epsilon^*(R, L) = \max_{\substack{P_{U|\hat{X}}, P_{\hat{X}|X}: \\ R \geq I(U;\hat{X}) \\ L \geq I(X;\hat{X})}} I(U;Y). \tag{21}$$

Then, for any $\epsilon \in [0, 1)$ and any $(R, L) \in \mathbb{R}_+^2$, the optimal error exponent for testing against independence when using a memoryless privacy mechanism is given by (21), where it suffices to choose $|\mathcal{U}| \leq |\hat{\mathcal{X}}| + 1$ and $|\hat{\mathcal{X}}| \leq |\mathcal{X}|$ according to Caratheodory's theorem [36] (Theorem 15.3.5).

Proof. The coding scheme is given in the following section. For the rest of proof, see Appendix B. □

4.2. Coding Scheme

In this section, we propose a coding scheme for Theorem 2. Fix the joint distribution as in (13), and the rate and privacy constraints as in (15). Generate the codebook $\mathcal{C}_U$ as in (16).

Randomizer: Upon observing x^n, it outputs the sequence $\hat{x}^n$ in which the i-th component $\hat{x}_i$ is generated based on x_i, according to $P_{\hat{X}|X}(\hat{x}_i|x_i)$.

Transmitter: It finds an index m such that $\left(u^n(m), \hat{x}^n\right) \in \mathcal{T}_{\mu/2}^n(P_{U\hat{X}})$. If successful, it sends the index m over the noiseless link to the receiver. Otherwise, it sends $m = 0$.

Receiver: Upon observing y^n and receiving the index m, if $m = 0$, the receiver declares $\hat{\mathcal{H}} = 1$. If $m \neq 0$, it checks whether $\left(u^n(m), y^n\right) \in \mathcal{T}_\mu^n(P_{UY})$. If the test is successful, the receiver declares $\hat{\mathcal{H}} = 0$; otherwise, it sets $\hat{\mathcal{H}} = 1$.

Remark 3. *In the above scheme, the sequence $\hat{X}^n$ is i.i.d. since it is generated based on the memoryless mechanism $P_{\hat{X}|X}$.*

When the communication rate is positive, there exists a trade-off between the optimal error exponent and the privacy criterion. The following example elucidates this trade-off.

4.3. Binary Example

In this section, we study hypothesis testing against independence for a binary example. Suppose that under both hypotheses, we have $X \sim \text{Bern}(\frac{1}{2})$. Under the null hypothesis,

$$\mathcal{H} = 0: \qquad Y = X \oplus N, \qquad N \sim \text{Bern}(q) \tag{22}$$

for some $0 \leq q \leq 1$, where N is independent of X. Under the alternative hypothesis

$$\mathcal{H} = 1: \qquad Y \sim \text{Bern}\left(\frac{1}{2}\right), \tag{23}$$

where Y is independent of X. The cardinality constraint shows that it suffices to choose $|\hat{\mathcal{X}}| = 2$. Among all possible privacy mechanisms, the choice of $P_{\hat{X}|X}(1|0) = P_{\hat{X}|X}(1|1)$ and $P_{\hat{X}|X}(0|0) = P_{\hat{X}|X}(0|1)$ minimizes the mutual information $I(X;\hat{X})$. Thus, we restrict to this choice which also results in $\hat{X} \sim \text{Bern}\left(\frac{1}{2}\right)$.

The cardinality bound on the auxiliary random variable U is $|\mathcal{U}| \leq 3$. The following proposition states that it is also optimal to choose $P_{U|\hat{X}}$ to be a BSC.

Proposition 1. *The optimal error exponent of the proposed binary setup is given by the following:*

$$\theta_\epsilon^*(R, L) = 1 - h_b\left(q \star h_b^{-1}(1 - L) \star h_b^{-1}(1 - R)\right). \tag{24}$$

Proof. For the proof of achievability, choose the following auxiliary random variables:

$$\hat{X} = X \oplus \hat{Z}, \qquad \hat{Z} \sim \text{Bern}(p_1) \tag{25}$$

$$U = \hat{X} \oplus Z, \qquad Z \sim \text{Bern}(p_2), \tag{26}$$

for some $0 \leq p_1, p_2 \leq 1$ where $\hat{Z}$ and Z are independent of X and $(X, \hat{X})$, respectively. The optimal error exponent of Theorem 2 reduces to the following:

$$\theta_\epsilon^*(R, L) = \max_{\substack{0 \leq p_1, p_2 \leq 1: \\ R \geq 1 - h_\text{b}(p_2) \\ L \geq 1 - h_\text{b}(p_1)}} 1 - h_\text{b}(q \star p_1 \star p_2), \tag{27}$$

which can be simplified to (24). For the proof of the converse, see Appendix C. □

Figure 2 illustrates the error exponent versus the privacy parameter L for a fixed rate R. There is clearly a trade-off between $\theta_\epsilon^*(R, L)$ and L. For a less stringent privacy requirement (large L), the error exponent $\theta_\epsilon^*(R, L)$ increases.

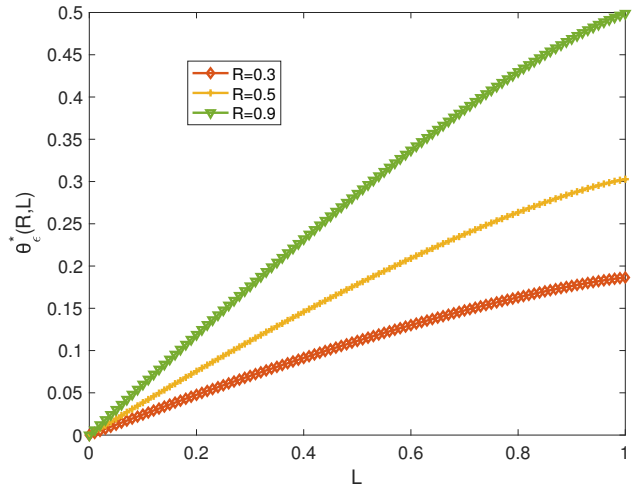

Figure 2. $\theta_\epsilon^*(R, L)$ versus L for $q = 0.1$ and various values of R.

4.4. Euclidean Approximation

In this section, we propose Euclidean approximations [30,31] for the optimal error exponent of testing against independence scenario (Theorem 2) when $R \approx 0$ and $L \approx 0$. Consider the optimal error exponent as follows:

$$\theta_\epsilon^*(R, L) = \max_{\substack{P_{U|\hat{X}}, P_{\hat{X}|X}: \\ R \geq I(U;\hat{X}) \\ L \geq I(X;\hat{X})}} I(U; Y). \tag{28}$$

Let $\mathbf{W}$ of dimension $|\mathcal{Y}| \times |\mathcal{X}|$, denote the transition matrix $P_{Y|X}$, which is itself induced by P_X and the joint distribution P_{XY}. Now, consider the rate constraint as follows:

$$I(U; \hat{X}) = \sum_{u \in \mathcal{U}} P_U(u) D\big(P_{\hat{X}|U}(\cdot|u) \| P_{\hat{X}}\big) \leq R. \tag{29}$$

Assuming $R \approx 0$, we let $P_{\hat{X}|U}(\cdot|u)$ be a local perturbation from $P_{\hat{X}}(\cdot)$, where we have

$$P_{\hat{X}|U}(\cdot|u) = P_{\hat{X}}(\cdot) + \psi_u(\cdot), \tag{30}$$

for a perturbation $\psi_u(\cdot)$ satisfying

$$\sum_{\hat{x}\in\hat{\mathcal{X}}} \psi_u(\hat{x}) = 0, \tag{31}$$

in order to preserve the row stochasticity of $P_{\hat{X}|U}$. Using a χ^2-approximation [30], we can write:

$$D\big(P_{\hat{X}|U}(\cdot|u)\|P_{\hat{X}}\big) \approx \frac{1}{2}\cdot \log e \cdot \|\mathbf{v}_u\|^2, \tag{32}$$

where $\mathbf{v}_u$ denotes the length-$|\hat{\mathcal{X}}|$ column vector of weighted perturbations whose $\hat{x}$-th component is defined as:

$$v_u(\hat{x}) \triangleq \frac{1}{\sqrt{P_{\hat{X}}(\hat{x})}}\cdot \psi_u(\hat{x}), \quad \forall \hat{x}\in\hat{\mathcal{X}}. \tag{33}$$

Using the above definition, the rate constraint in (29) can be written as:

$$\sum_{u\in\mathcal{U}} P_U(u)\,\|\mathbf{v}_u\|^2 \le \frac{2R}{\log e}. \tag{34}$$

Similarly, consider the privacy constraint as the following:

$$I(X;\hat{X}) = \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}}(\hat{x}) D\big(P_{X|\hat{X}}(\cdot|\hat{x})\|P_X\big) \le L. \tag{35}$$

Assuming $L \approx 0$, we let $P_{X|\hat{X}}(\cdot|\hat{x})$ be a local perturbation from $P_X(\cdot)$ where

$$P_{X|\hat{X}}(\cdot|\hat{x}) = P_X(\cdot) + \phi_{\hat{x}}(\cdot), \tag{36}$$

for a perturbation $\phi_{\hat{x}}(\cdot)$ that satifies:

$$\sum_{x\in\mathcal{X}} \phi_{\hat{x}}(x) = 0. \tag{37}$$

Again, using a χ^2-approximation, we obtain the following:

$$D\big(P_{X|\hat{X}}(\cdot|\hat{x})\|P_X\big) \approx \frac{1}{2}\,\log e\,\,\|\mathbf{v}_{\hat{x}}\|^2, \tag{38}$$

where $\mathbf{v}_{\hat{x}}$ is a length-$|\mathcal{X}|$ column vector and its x-th component is defined as follows:

$$v_{\hat{x}}(x) \triangleq \frac{1}{\sqrt{P_X(x)}}\cdot \phi_{\hat{x}}(x), \quad \forall x\in\mathcal{X}. \tag{39}$$

Thus, the privacy constraint in (35) can be written as:

$$\sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}}(\hat{x})\,\|\mathbf{v}_{\hat{x}}\|^2 \le \frac{2L}{\log e}. \tag{40}$$

For any $x\in\mathcal{X}$ and $u\in\mathcal{U}$, we define the following:

$$\Lambda_u(x) \triangleq \sum_{\hat{x}\in\hat{\mathcal{X}}} \psi_u(\hat{x})\,\phi_{\hat{x}}(x) \tag{41}$$

$$= \sqrt{P_X(x)} \sum_{\hat{x}\in\hat{\mathcal{X}}} \sqrt{P_{\hat{X}}(\hat{x})}\; v_u(\hat{x})\; v_{\hat{x}}(x), \tag{42}$$

and the corresponding length-$|\mathcal{X}|$ column vector $\mathbf{\Lambda}_u$ defined as follows:

$$\mathbf{\Lambda}_u = \left[\sqrt{P_X}\right] \mathbf{V}_{\hat{X}} \left[\sqrt{P_{\hat{X}}}\right] \mathbf{v}_u, \tag{43}$$

where $\left[\sqrt{P_X}\right]$ denotes a diagonal $|\mathcal{X}| \times |\mathcal{X}|$-matrix, so that its (x,x)-th element ($x \in \mathcal{X}$) is $\sqrt{P_X(x)}$, and $\left[\sqrt{P_{\hat{X}}}\right]$ is defined similarly. Moreover, $\mathbf{V}_{\hat{X}}$ refers to the $|\mathcal{X}| \times |\hat{\mathcal{X}}|$-matrix defined as follows:

$$\mathbf{V}_{\hat{X}} \triangleq \begin{bmatrix} \mathbf{v}_1 & \mathbf{v}_2 & \dots & \mathbf{v}_{\hat{x}} & \dots & \mathbf{v}_{|\hat{\mathcal{X}}|} \end{bmatrix}. \tag{44}$$

Let $\left[\sqrt{P_Y}\right]^{-1}$ be the inverse of diagonal $|\mathcal{Y}| \times |\mathcal{Y}|$-matrix $\left[\sqrt{P_Y}\right]$. As shown in Appendix D, the optimization problem in (28) can be written as follows:

$$\max_{\substack{\{\mathbf{v}_u\}_{u\in\mathcal{U}}, \mathbf{V}_{\hat{X}}: \\ -\sqrt{P_{\hat{X}}(\hat{x})} \le \mathbf{v}_u(\hat{x}) \le \frac{1-P_{\hat{X}}(\hat{x})}{\sqrt{P_{\hat{X}}(\hat{x})}} \\ -\sqrt{P_X(x)} \le \mathbf{v}_{\hat{x}}(x) \le \frac{1-P_X(x)}{\sqrt{P_X(x)}}}} \quad \frac{1}{2} \log e \left[\sum_{u\in\mathcal{U}} P_U(u) \cdot \left\| \left[\sqrt{P_Y}\right]^{-1} \mathbf{W} \left[\sqrt{P_X}\right] \mathbf{V}_{\hat{X}} \left[\sqrt{P_{\hat{X}}}\right] \mathbf{V}_u \right\|^2 \right] \tag{45}$$

$$\text{subject to:} \quad \sum_{u\in\mathcal{U}} P_U(u) \left\|\mathbf{v}_u\right\|^2 \le \frac{2R}{\log e}, \tag{46}$$

$$\sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}}(\hat{x}) \left\|\mathbf{v}_{\hat{x}}\right\|^2 \le \frac{2L}{\log e}. \tag{47}$$

The following example specializes the above approximation to the binary case.

Example 1. *Consider the binary setup of Example 4.3 and the choice of auxiliary random variables in (26). Since the privacy mechanism is assumed to be a BSC, we have*

$$\mathbf{P}_X = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \end{bmatrix}^T, \qquad \mathbf{P}_{\hat{X}} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \end{bmatrix}^T, \tag{48}$$

Now, we consider the vectors $\mathbf{v}_{u=0}$ and $\mathbf{v}_{u=1}$ defined as

$$\mathbf{v}_{u=0} = \begin{bmatrix} \sqrt{2}\xi_1 & -\sqrt{2}\xi_1 \end{bmatrix}^T, \tag{49}$$

$$\mathbf{v}_{u=1} = \begin{bmatrix} -\sqrt{2}\xi_1 & \sqrt{2}\xi_1 \end{bmatrix}^T. \tag{50}$$

for some positive ξ_1. This yields the following:

$$\mathbf{P}_{\hat{X}|U=0} = \mathbf{P}_{\hat{X}} + \begin{bmatrix} \xi_1 & -\xi_1 \end{bmatrix}^T, \tag{51}$$

$$\mathbf{P}_{\hat{X}|U=1} = \mathbf{P}_{\hat{X}} + \begin{bmatrix} -\xi_1 & \xi_1 \end{bmatrix}^T \tag{52}$$

We also choose the vectors $\mathbf{v}_{\hat{x}=0}$ and $\mathbf{v}_{\hat{x}=1}$ as follows:

$$\mathbf{v}_{\hat{x}=0} = \begin{bmatrix} \sqrt{2}\xi_2 & -\sqrt{2}\xi_2 \end{bmatrix}^T, \tag{53}$$

$$\mathbf{v}_{\hat{x}=1} = \begin{bmatrix} -\sqrt{2}\xi_2 & \sqrt{2}\xi_2 \end{bmatrix}^T, \tag{54}$$

which results in

$$\mathbf{P}_{X|\hat{X}=0} = \mathbf{P}_X + \begin{bmatrix} \xi_2 & -\xi_2 \end{bmatrix}^T, \tag{55}$$

$$\mathbf{P}_{X|\hat{X}=1} = \mathbf{P}_X + [-\xi_2 \quad \xi_2]^T. \tag{56}$$

Notice that the matrix $\mathbf{W}$ *is given by*

$$\mathbf{W} = \begin{bmatrix} 1-q & q \\ q & 1-q \end{bmatrix}. \tag{57}$$

Thus, the optimization problem in (45) *and* (47) *reduces to the following:*

$$\max_{-\frac{1}{2} \le \xi_1, \xi_2 \le \frac{1}{2}} \quad 8 \log e \, (1-2q)^2 \, |\xi_1|^2 \, |\xi_2|^2 \tag{58}$$

$$\text{subject to:} \quad 4\,|\xi_1|^2 \le \frac{2R}{\log e} \quad \text{and} \quad 4\,|\xi_2|^2 \le \frac{2L}{\log e}. \tag{59}$$

Solving the above optimization yields

$$\theta_\epsilon^*(R \approx 0, L \approx 0) \approx \frac{2}{\log e} \, (1-2q)^2 \, R \, L. \tag{60}$$

For some values of parameters, the approximation in (60) *is compared to the error exponent of* (24) *in Figure 3. We observe that when* $R = L \approx 0$*, the approximation turns out to be excellent.*

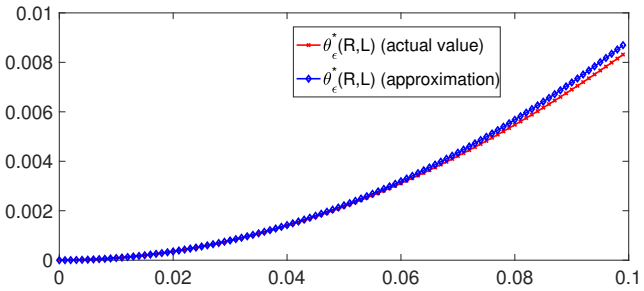

Figure 3. $\theta_\epsilon^*(R \approx 0, L \approx 0)$ versus L for $q = 0.1$ and $R = L$.

Remark 4. *The trade-off between the optimal error exponent and the privacy can again be verified from* (60) *in the case of* $L \approx 0$ *and* $R \approx 0$*. As* L *becomes larger (which corresponds to a less stringent privacy requirement), the error exponent also increases. For a fixed error exponent, a trade-off between* R *and* L *exists. An increase in* R *results in a decrease of* L*.*

4.5. Gaussian Setup

In this section, we consider hypothesis testing against independence over a Gaussian example. Suppose that $X \sim \mathcal{N}(0,1)$ and under the null hypothesis $\mathcal{H} = 0$, the sources X and Y are jointly Gaussian random variables distributed as $\mathcal{N}(0, \mathbf{G}_{XY})$, where $\mathbf{G}_{XY}$ is defined as the following:

$$\mathbf{G}_{XY} \stackrel{\Delta}{=} \begin{bmatrix} 1 & \rho \\ \rho & 1 \end{bmatrix}, \tag{61}$$

for some $0 \le \rho \le 1$.

Under the alternative hypothesis $\mathcal{H} = 1$, we assume that X and Y are independent Gaussian random variables, each distributed as $\mathcal{N}(0,1)$. Consider the privacy constraint as follows:

$$L \ge I(X;\hat{X}) = h(X) - h(X|\hat{X}). \tag{62}$$

For a Gaussian source X, the conditional entropy $h(X|\hat{X})$ is maximized for a jointly Gaussian $(X, \hat{X})$. This choice minimizes the RHS of (62). Thus, without loss of optimality, we choose

$$X = \hat{X} + Z, \qquad Z \sim \mathcal{N}\left(0, 2^{-2L}\right), \tag{63}$$

where Z is independent of $\hat{X}$. The following proposition states that it is optimal to choose U jointly Gaussian with $(X, \hat{X}, Y)$.

Proposition 2. *The optimal error exponent of the proposed Gaussian setup is given by*

$$\theta_\epsilon^*(R, L) = \frac{1}{2} \log \left(\frac{1}{1 - \rho^2 \cdot (1 - 2^{-2R}) \cdot (1 - 2^{-2L})} \right). \tag{64}$$

Proof. For the proof of achievability, we choose $\hat{X}$ as in (63). Also, let

$$\hat{X} = U + \hat{Z}, \qquad \hat{Z} \sim \mathcal{N}(0, \beta^2), \tag{65}$$

for some $\beta^2 \geq 0$, where $\hat{Z}$ is independent of U. It can be shown that Theorem 2 remains valid when it is extended to the continuous alphabet [5]. For the details of the simplification and also the proof of converse, see Appendix E. □

Remark 5. *If $L = \infty$, the above proposition recovers the optimal error exponent of Rahman and Wagner [5] (Corollary 7) for testing against independence of Gaussian sources over a noiseless link of rate R.*

5. Summary and Discussion

In this paper, distributed hypothesis testing with privacy constraints is considered. A coding scheme is proposed where the sensor decides on one of hypotheses and generates the randomized data based on its decision. The transmitter describes the randomized data over a noiseless link to the receiver. The privacy mechanism in this scheme is non-memoryless. The special case of testing against independence with a memoryless privacy mechanism is studied in detail. The optimal type-II error exponent of this case is established, together with a strong converse. A binary example is proposed where the trade-off between the privacy criterion and the error exponent is reported. Euclidean approximations are provided for the case in which the privacy level is high and and the communication rate is vanishingly small. The optimal type-II error exponent of a Gaussian setup is also established.

A future line of research is to study the second-order asymptotics of our model. The second-order analysis of distributed hypothesis testing without privacy constraints and with zero-rate communication was studied in [37]. In our proposed model, the trade-off between the privacy and type-II error exponent is observed, i.e., a less stringent privacy requirement yields a larger error exponent. The next step is to see whether the trade-off between privacy and error exponent affects the second-order term.

Another potential line for future research is to consider other metrics of privacy instead of the mutual information. A possible candidate is to use the maximal leakage [21–23] and to analyze the performance in tandem with distributed hypothesis testing problem.

Author Contributions: Investigation, A.G.; Supervision, S.S. and V.Y.F.T.; Writing—original draft, S.B.A.

Funding: This research was partially funded by grants R-263-000-C83-112 and R-263-000-C54-114.

Acknowledgments: The authors would like to thank Lin Zhou (National University of Singapore) and Daming Cao (Southeast University) for helpful discussions during the preparation of the manuscript.

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

Appendix A. Proof of Theorem 1

The analysis is based on the scheme described in Section 3.2.

Error Probability Analysis: We analyze the type-I and type-II error probabilities averaged over all random codebooks. By standard arguments [36] (p. 204), it can be shown that there exists at least one codebook that satisfies constraints on the error probabilities.

For the considered $\mu > 0$ and the considered blocklength n, let $\mathcal{P}_\mu^n$ be the set of all joint types $\pi_{U\hat{X}XY}$ over $\mathcal{U}^n \times \hat{\mathcal{X}}^n \times \mathcal{X}^n \times \mathcal{Y}^n$ which satisfy the following constraints:

$$\left|\pi_X - P_X\right| \leq \mu/4, \tag{A1}$$

$$\left|\pi_{U\hat{X}} - P_{U\hat{X}}\right| \leq \mu/2, \tag{A2}$$

$$\left|\pi_{UY} - P_{UY}\right| \leq \mu. \tag{A3}$$

First, we analyze the type-I error probability. For the case of $M \neq 0$, we define the following event:

$$\mathcal{E} \triangleq \left\{(U^n(M), Y^n) \notin \mathcal{T}_\mu^n(P_{UY})\right\}. \tag{A4}$$

Thus, type-I error probability can be upper bounded as follows:

$$\begin{aligned}
\alpha_n &\leq \Pr\left[\hat{X}^n = 0^n \text{ or } M = 0 \text{ or } \mathcal{E} \,\middle|\, \mathcal{H} = 0\right] && \text{(A5)}\\
&\leq \Pr\left[\hat{X}^n = 0^n \,\middle|\, \mathcal{H} = 0\right] + \Pr\left[M = 0 \,\middle|\, \hat{X}^n \neq 0^n, \mathcal{H} = 0\right] + \Pr\left[\mathcal{E} \,\middle|\, M \neq 0, \hat{X}^n \neq 0^n, \mathcal{H} = 0\right] && \text{(A6)}\\
&\leq \epsilon/3 + \Pr\left[M = 0 \,\middle|\, \hat{X}^n \neq 0^n, \mathcal{H} = 0\right] + \Pr\left[\mathcal{E} \,\middle|\, M \neq 0, \hat{X}^n \neq 0^n, \mathcal{H} = 0\right] && \text{(A7)}\\
&\leq \epsilon/3 + \epsilon/3 + \Pr\left[\mathcal{E} \,\middle|\, M \neq 0, \hat{X}^n \neq 0^n, \mathcal{H} = 0\right] && \text{(A8)}\\
&\leq \epsilon/3 + \epsilon/3 + \epsilon/3 && \text{(A9)}\\
&= \epsilon, && \text{(A10)}
\end{aligned}$$

where (A7) follows from AEP [36] (Theorem 3.1.1); (A8) follows from the covering lemma [34] (Lemma 3.3) and the rate constraint (15), (A10) follows from Markov lemma [34] (Lemma 12.1). In all justifications, n is taken to be sufficiently large.

Next, we analyze the type-II error probability. The acceptance region at the receiver is

$$\mathcal{A}_n^{\mathrm{Rx}} = \bigcup_m \left\{ (\hat{x}^n, x^n, y^n) : \hat{x}^n \neq 0^n, (u^n(m), \hat{x}^n, x^n, y^n) \in \mathcal{T}_\mu^n(P_{U\hat{X}XY}) \right\}. \tag{A11}$$

The set $\mathcal{A}_n^{\mathrm{Rx}}$ is contained within the following acceptance region $\bar{\mathcal{A}}_n$:

$$\bar{\mathcal{A}}_n = \bigcup_m \left\{ (\hat{x}^n, x^n, y^n) : \hat{x}^n \neq 0^n, (u^n(m), \hat{x}^n, x^n, y^n) \in \bigcup_{\pi \in \mathcal{P}_\mu^n} \mathcal{T}^n(\pi) \right\}. \tag{A12}$$

Let $\mathcal{F}_m \triangleq \{(U^n(m), \hat{X}^n, X^n, Y^n) \in \mathcal{P}_\mu^n\}$. Therefore, the average of type-II error probability over all codebooks is upper bounded as follows:

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}}[\beta_n] &\leq Q_{\hat{X}XY}^n(\bar{\mathcal{A}}_n) && \text{(A13)}\\
&\leq \sum_m \Pr\left[\hat{X}^n \neq 0^n, \mathcal{F}_m \,\middle|\, \mathcal{H} = 1\right] && \text{(A14)}\\
&\leq \sum_m \Pr\left[\mathcal{F}_m \,\middle|\, \hat{X}^n \neq 0^n, \mathcal{H} = 1\right] && \text{(A15)}\\
&\leq 2^{nR} \cdot (n+1)^{|\mathcal{U}|\cdot|\hat{\mathcal{X}}|\cdot|\mathcal{X}|\cdot|\mathcal{Y}|} \cdot \max_{\pi_{U\hat{X}XY} \in \mathcal{P}_\mu^n} 2^{-nD(\pi_{U\hat{X}XY} \| P_U P_{\hat{X}|X} Q_{XY})} && \text{(A16)}
\end{aligned}$$

$$= (n+1)^{|\mathcal{U}|\cdot|\hat{\mathcal{X}}|\cdot|\mathcal{X}|\cdot|\mathcal{Y}|} \cdot 2^{-n\tilde{\theta}_\mu}, \tag{A17}$$

where

$$\tilde{\theta}_\mu \triangleq \min_{\pi_{U\hat{X}XY}\in\mathcal{P}_\mu^n} D(\pi_{U\hat{X}XY}\|P_U P_{\hat{X}|X} Q_{XY}) - R, \tag{A18}$$

and (A16) follows from the upper bound of Sanov's theorem [36] (Theorem 11.4.1). Hence,

$$\tilde{\theta}_\mu = \min_{\pi_{U\hat{X}XY}\in\mathcal{P}_\mu^n} D(\pi_{U\hat{X}XY}\|P_U P_{\hat{X}|X} Q_{XY}) - R \tag{A19}$$

$$= \min_{\pi_{U\hat{X}XY}\in\mathcal{P}_\mu^n} D(\pi_{U\hat{X}XY}\|P_U P_{\hat{X}|X} Q_{XY}) - I(U;\hat{X}) - \mu \tag{A20}$$

$$= \min_{\pi_{U\hat{X}XY}\in\mathcal{P}_\mu^n} D(\pi_{U\hat{X}XY}\|P_{U|\hat{X}} P_{\hat{X}|X} Q_{XY}) + \delta(\mu), \tag{A21}$$

where $\delta(\mu) \to 0$ as $\mu \to 0$. Equality (A20) follows from the rate constraint in (15) and (A21) holds because $|\pi_{U\hat{X}} - P_{U\hat{X}}| < \mu/2$.

Privacy Analysis: We first analyze the privacy under $\mathcal{H} = 0$. Notice that $\hat{X}^n$ is not necessarily i.i.d. because according to the scheme in Section 3.2, $\hat{X}^n$ is forced to be an all-zero sequence if the Randomizer decides that X^n is not typical. However, conditioned on the event that $X^n \in \mathcal{T}_\mu^n(P_X)$, the sequence $\hat{X}^n$ is i.i.d. according to the conditional pmf $P_{\hat{X}|X}$. The privacy measure T_n satisfies

$$nT_n = I(X^n;\hat{X}^n) = H(\hat{X}^n) - H(\hat{X}^n|X^n). \tag{A22}$$

We now provide a lower bound on $H(\hat{X}^n|X^n)$ as follows

$$H(\hat{X}^n|X^n) \geq \sum_{x^n\in\mathcal{T}_\mu^n(P_X)} P_X^n(x^n) H(\hat{X}^n|X^n = x^n) \tag{A23}$$

For any $x^n \in \mathcal{T}_\mu^n(P_X)$ and for $\mu' > \mu$, it holds that

$$H(\hat{X}^n|X^n = x^n) = -\sum_{\hat{x}^n\in\hat{\mathcal{X}}^n} P_{\hat{X}|X}^n(\hat{x}^n|x^n) \log P_{\hat{X}|X}^n(\hat{x}^n|x^n) \tag{A24}$$

$$\geq -\sum_{\hat{x}^n\in\mathcal{T}_{\mu'}^n(P_{\hat{X}|X}(\cdot|x^n))} P_{\hat{X}|X}^n(\hat{x}^n|x^n) \log P_{\hat{X}|X}^n(\hat{x}^n|x^n) \tag{A25}$$

$$\geq -\sum_{\hat{x}^n\in\mathcal{T}_{\mu'}^n(P_{\hat{X}|X}(\cdot|x^n))} P_{\hat{X}|X}^n(\hat{x}^n|x^n) \log \left[2^{-n(1-\mu')H(\hat{X}|X)}\right] \tag{A26}$$

$$\geq n(1-\mu')^2 H(\hat{X}|X) \tag{A27}$$

where (A26) is true because for any $\hat{x}^n \in \mathcal{T}_{\mu'}^n(P_{\hat{X}|X}(\cdot|x^n))$, it holds that $P_{\hat{X}|X}^n(\hat{x}^n|x^n) \leq 2^{-n(1-\mu')H(\hat{X}|X)}$, and (A27) follows because the conditional typicality lemma [34] (Chapter 2) implies that $P_{\hat{X}|X}^n(\mathcal{T}_{\mu'}^n(P_{\hat{X}|X}(\cdot|x^n))|x^n) \geq 1-\mu'$ for n sufficiently large.

Combining (A23) and (A27), we obtain

$$H(\hat{X}^n|X^n) \geq n(1-\mu')^2 H(\hat{X}|X) \sum_{x^n\in\mathcal{T}_\mu^n(P_X)} P_X^n(x^n) \tag{A28}$$

$$\geq n(1-\mu')^2(1-\mu) H(\hat{X}|X), \tag{A29}$$

where (A29) follows because the AEP [36] (Theorem 3.1.1) implies that $P_X^n(\mathcal{T}_\mu^n(P_X)) \geq 1-\mu$ for n sufficiently large.

Hence, we have

$$I(X^n;\hat{X}^n) = H(\hat{X}^n) - H(\hat{X}^n|X^n) \tag{A30}$$
$$\leq nH(\hat{X}) - H(\hat{X}^n|X^n) \tag{A31}$$
$$\leq nH(\hat{X}) - n(1-\mu'')H(\hat{X}|X) \tag{A32}$$
$$= nI(X;\hat{X}) + n\mu''H(\hat{X}|X) \tag{A33}$$
$$\leq nL + n\mu'' \cdot \log|\hat{\mathcal{X}}| \tag{A34}$$
$$= nL + n\zeta, \tag{A35}$$

where $\mu'' \triangleq 1-(1-\mu')^2(1-\mu) \geq 0$, and $\zeta \triangleq \mu'' \cdot \log|\hat{\mathcal{X}}|$.

Next, consider the privacy analysis under $\mathcal{H}=1$. Please note that when $P_X = Q_X$, the analysis is similar to that of $\mathcal{H}=0$. Thus, we assume that $P_X \neq Q_X$ in the following. From (A22), the privacy measure T_n satisfies:

$$nT_n = I(X^n;\hat{X}^n) \leq H(\hat{X}^n). \tag{A36}$$

To upper bound $H(\hat{X}^n)$, we calculate the probability $P_{\hat{X}^n}(\hat{x}^n)$ for $\hat{x}^n = 0^n$ as follows:

$$P_{\hat{X}^n}(0^n) = \sum_{x^n \in \mathcal{T}_\mu^n(P_X)} P_{\hat{X}|X}^n(0^n|x^n)\cdot Q_X^n(x^n) + \sum_{x^n \notin \mathcal{T}_\mu^n(P_X)} P_{\hat{X}|X}^n(0^n|x^n)\cdot Q_X^n(x^n) \tag{A37}$$
$$= \sum_{x^n \notin \mathcal{T}_\mu^n(P_X)} P_{\hat{X}|X}^n(0^n|x^n)\cdot Q_X^n(x^n) \tag{A38}$$
$$= \sum_{x^n \notin \mathcal{T}_\mu^n(P_X)} Q_X^n(x^n) \tag{A39}$$
$$= 1 - Q_X^n\left(\mathcal{T}_\mu^n(P_X)\right) \tag{A40}$$
$$\geq 1 - 2^{-n(D(P_X\|Q_X)+\delta(\mu))} \triangleq 1-\gamma_n, \tag{A41}$$

where $\gamma_n \to 0$ exponentially fast as $n \to \infty$. Here, (A38) follows because if $x^n \in \mathcal{T}_\mu^n(P_X)$, then $P_{\hat{X}|X}^n(0^n|x^n) = 0$, (A39) follows because when $x^n \notin \mathcal{T}_\mu^n(P_X)$, then $P_{\hat{X}|X}^n(0^n|x^n) = 1$ and (A41) follows from Sanov's theorem and the continuity of the relative entropy in its first argument [38] (Lemma 1.2.7).

Write $H(\hat{X}^n)$ as $H(P_{\hat{X}^n})$ and let P_{0^n} be the distribution on $\hat{\mathcal{X}}^n$ that places all its probability mass on $0^n \in \hat{\mathcal{X}}^n$. Since $H(P_{0^n}) = 0$, by the uniform continuity of entropy [38] (Lemma 1.2.7),

$$H(P_{\hat{X}^n}) \leq 2\left|P_{\hat{X}^n} - P_{0^n}\right| \cdot \log \frac{|\hat{\mathcal{X}}|^n}{2\left|P_{\hat{X}^n} - P_{0^n}\right|}. \tag{A42}$$

Since $\gamma_n \to 0$ exponentially fast, the same holds true for $|P_{\hat{X}^n} - P_{0^n}|$ and so by (A42), $H(P_{\hat{X}^n}) = H(\hat{X}^n) \to 0$. Therefore, under $\mathcal{H}=1$, we have $T_n \to 0$ as $n \to \infty$.

Letting $n \to \infty$ and then letting $\mu, \mu', \gamma \to 0$, we obtain $\tilde{\theta}_\mu \to \theta$ and $\limsup_{n\to n} T_n \leq L$, with θ given by the RHS of (11). This establishes the proof of Theorem 1.

Appendix B. Proof of Theorem 2

Achievability: The analysis is based on the scheme of Section 4.2. It follows similar steps as in [1]. Recall the definition of the event $\mathcal{E}$ in (A4). Consider the type-I error probability as follows:

$$\alpha_n \leq \Pr\left[M=0 \text{ or } \mathcal{E}\middle|\mathcal{H}=0\right] \tag{A43}$$
$$\leq \Pr\left[M=0\middle|\mathcal{H}=0\right] + \Pr\left[\mathcal{E}\middle|M\neq 0,\mathcal{H}=0\right] \tag{A44}$$
$$\leq \epsilon/2 + \epsilon/2 \tag{A45}$$
$$= \epsilon, \tag{A46}$$

where (A46) follows from covering lemma [34] (Lemma 3.3) and the rate constraint in (15), and also the Markov lemma [34] (Lemma 12.1). Now, consider the type-II error probability as follows:

$$\begin{aligned}\beta_n &= \Pr[\hat{\mathcal{H}} = 0 | \mathcal{H} = 1] && \text{(A47)}\\ &= \Pr[\hat{\mathcal{H}} = 0, M \neq 0 | \mathcal{H} = 1] && \text{(A48)}\\ &\leq \Pr[\hat{\mathcal{H}} = 0 | \mathcal{H} = 1, M \neq 0] && \text{(A49)}\\ &= \Pr[\hat{\mathcal{H}} = 0 | \mathcal{H} = 1, M = 1], && \text{(A50)}\end{aligned}$$

where the last equality follows from the symmetry of the code construction. Now, the average of type-II error probability over all codebooks satisfies:

$$\mathbb{E}_{\mathcal{C}}\left[\beta_n\right] \leq 2^{-n[I(U;Y)-\delta(\mu)]}, \tag{A51}$$

where $\delta(\mu)$ is a function that tends to zero as $\mu \to 0$. The privacy analysis is straightforward since the privacy mechanism is memoryless whence we have

$$\frac{1}{n} I(X^n; \hat{X}^n) = I(X; \hat{X}) = L + \zeta, \tag{A52}$$

where the last equality follows from the privacy constraint in (15). This concludes the proof of achievability.

Converse: Now, we prove the strong converse. It involves an extension of the η-image characterization technique [4,38]. The proof steps are given as follows. First, we find a truncated distribution $P_{\underline{\hat{X}}^n}$ which is arbitrarily close to $P^n_{\hat{X}}$ in terms of entropy. Then, we analyze the type-II error probability under a constrained type-I error probability. Finally, a single-letter characterization of the rate and privacy constraints is given.

(1) *Construction of a Truncated Distribution:*

Since the privacy machanism is memoryless, we conclude that $(X^n, \hat{X}^n, Y^n)$ is i.i.d. according to $P_{X\hat{X}Y} \triangleq P_{\hat{X}|X} P_{XY}$. For a given $P_{\hat{X}Y}$, define $V^n(y^n|\hat{x}^n) \triangleq P^n_{Y|\hat{X}}(y^n|\hat{x}^n)$ for all $\hat{x}^n \in \hat{\mathcal{X}}^n$ and $y^n \in \mathcal{Y}^n$. A set $B \subseteq \mathcal{Y}^n$ is an η-image of the set $A \subseteq \hat{\mathcal{X}}^n$ over the channel V^n if

$$V^n\left(B|\hat{x}^n\right) \geq \eta, \quad \forall \hat{x}^n \in A. \tag{A53}$$

The privacy mechanism is the same under both hypotheses, thus, we can define the acceptance region based on $(\hat{x}^n, y^n)$ as follows:

$$rCl\mathcal{A}_n \triangleq \left\{(\hat{x}^n, y^n) \colon g^{(n)}(y^n, \phi^{(n)}(\hat{x}^n)) = 0\right\}. \tag{A54}$$

For any encoding function $\phi^{(n)}$ and an acceptance region $\mathcal{A}_n \subseteq \hat{\mathcal{X}}^n \times \mathcal{Y}^n$, let τ_n denote the cardinality of codebook and define the following sets:

$$C_i \stackrel{\Delta}{=} \left\{\hat{x}^n \in \hat{\mathcal{X}}^n \colon \phi^{(n)}(\hat{x}^n) = i\right\}, \tag{A55}$$

$$D_i \stackrel{\Delta}{=} \left\{y^n \in \mathcal{Y}^n \colon g^{(n)}(y^n, i) = 0\right\}, \quad 1 \leq i \leq \tau_n. \tag{A56}$$

The acceptance region can be written as follows:

$$\mathcal{A}_n = \bigcup_{i=1}^{\tau_n} \left(C_i \times D_i\right), \tag{A57}$$

where $C_i \cap C_j = \phi$ for all $i \neq j$. Define the set $\mathcal{B}_n(\eta)$ as follows:

$$\mathcal{B}_n(\eta) \triangleq \left\{\hat{x}^n \colon V^n\left(D_{\phi^{(n)}(\hat{x}^n)}|\hat{x}^n\right) \geq \eta\right\}. \tag{A58}$$

Fix $\epsilon \in [0,1)$ and notice that the type-I error probability is upper-bounded as

$$\alpha_n = P^n_{\hat{X}Y}\left(\mathcal{A}_n^c\right) \leq \epsilon, \tag{A59}$$

which we can write equivalently as

$$\begin{aligned} 1-\epsilon &\leq P^n_{\hat{X}Y}\left(\mathcal{A}_n\right) && \text{(A60)}\\ &= \sum_{\hat{x}^n \in \mathcal{B}_n(\eta)} P^n_{\hat{X}}(\hat{x}^n) V^n\left(D_{\phi^{(n)}(\hat{x}^n)}|\hat{x}^n\right) + \sum_{\hat{x}^n \in \mathcal{B}_n^c(\eta)} P^n_{\hat{X}}(\hat{x}^n) V^n\left(D_{\phi^{(n)}(\hat{x}^n)}|\hat{x}^n\right) && \text{(A61)}\\ &\leq P^n_{\hat{X}}\left(\mathcal{B}_n(\eta)\right) + \eta\left(1 - P^n_{\hat{X}}(\mathcal{B}_n(\eta))\right), && \text{(A62)} \end{aligned}$$

where the first term is because $V^n\left(D_{\phi^{(n)}(\hat{x}^n)}|\hat{x}^n\right) \leq 1$; and the second term is because for any $\hat{x}^n \in \mathcal{B}_n^c(\eta)$, we have $V^n\left(D_{\phi^{(n)}(\hat{x}^n)}|\hat{x}^n\right) < \eta$.

In what follows, let $\eta = \frac{1-\epsilon}{2}$. Inequality (A62) implies

$$P^n_{\hat{X}}(\mathcal{B}_n(\eta)) \geq \frac{1-\epsilon}{1+\epsilon}. \tag{A63}$$

Let $\mu_n = n^{-1/3}$. For the typical set $\mathcal{T}^n_{\mu_n}(P_{\hat{X}})$, we have

$$P^n_{\hat{X}}\left(\mathcal{T}^n_{\mu_n}(P_{\hat{X}})\right) \geq 1 - \frac{|\hat{\mathcal{X}}|}{2\mu_n n}. \tag{A64}$$

Hence,

$$\begin{aligned} P^n_{\hat{X}}\Big(\mathcal{T}^n_{\mu_n}(P_{\hat{X}}) \cap \mathcal{B}_n(\eta)\Big) &\geq P^n_{\hat{X}}\left(\mathcal{T}^n_{\mu_n}(P_{\hat{X}})\right) + P^n_{\hat{X}}\left(\mathcal{B}_n(\eta)\right) - 1 && \text{(A65)}\\ &\geq \frac{1-\epsilon}{1+\epsilon} - \frac{|\hat{\mathcal{X}}|}{2\mu_n n}. && \text{(A66)} \end{aligned}$$

For any $0 < \delta < \frac{1-\epsilon}{1+\epsilon}$ and for sufficiently large n,

$$P^n_{\hat{X}}\left(\mathcal{T}^n_{\mu_n}(P_{\hat{X}}) \cap \mathcal{B}_n(\eta)\right) \geq \delta. \tag{A67}$$

We can also write $\mathcal{T}^n_{\mu_n}(P_{\hat{X}})$ as

$$\mathcal{T}^n_{\mu_n}(P_{\hat{X}}) = \bigcup_{\hat{P}_{\hat{X}} : |\hat{P}_{\hat{X}} - P_{\hat{X}}| \leq \mu_n} \mathcal{T}^n(\hat{P}_{\hat{X}}). \tag{A68}$$

Combining the above equations, we get

$$\sum_{\hat{P}_{\hat{X}} : |\hat{P}_{\hat{X}} - P_{\hat{X}}| \leq \mu_n} P^n_{\hat{X}}\left(\mathcal{T}^n(\hat{P}_{\hat{X}}) \cap \mathcal{B}_n(\eta)\right) \geq \delta. \tag{A69}$$

Let $\tilde{P}_{\hat{X}}$ denote the type which maximizes the $P_{\hat{X}}^n$-probability of the type class among all such types. As there exist at most $(n+1)^{|\hat{\mathcal{X}}|}$ possible types, it holds that

$$P_{\hat{X}}^n\left(\mathcal{T}^n(\tilde{P}_{\hat{X}}) \cap \mathcal{B}_n(\eta)\right) \geq \frac{\delta}{(n+1)^{|\hat{\mathcal{X}}|}}. \tag{A70}$$

Define the set $\Psi_n(\eta) \triangleq \mathcal{T}^n(\tilde{P}_{\hat{X}}) \cap \mathcal{B}_n(\eta)$. We can write the probability in (A70) as

$$P_{\hat{X}}^n\left(\mathcal{T}^n(\tilde{P}_{\hat{X}}) \cap \mathcal{B}_n(\eta)\right) = \sum_{\hat{x}^n \in \Psi_n(\eta)} P_{\hat{X}}^n(\hat{x}^n) \tag{A71}$$

$$= \sum_{\hat{x}^n \in \Psi_n(\eta)} 2^{-n\left[D(\tilde{P}_{\hat{X}}\|P_{\hat{X}}) + H_{\tilde{P}_{\hat{X}}}(\hat{X})\right]} \tag{A72}$$

$$\leq \sum_{\hat{x}^n \in \Psi_n(\eta)} 2^{-n[H(\hat{X}) - \delta_1]} \tag{A73}$$

where $\delta_1 \to 0$ as $n \to \infty$ due to the fact that $D(\tilde{P}_{\hat{X}}\|P_{\hat{X}}) \geq 0$ and $|\tilde{P}_{\hat{X}} - P_{\hat{X}}| \leq \mu_n$ so the entropies are also arbitrarily close. It then follows from (A70) and (A73) that

$$\frac{1}{n}\log|\Psi_n(\eta)| \geq H(\hat{X}) - \delta_2, \tag{A74}$$

where $\delta_2 \to 0$ as $\mu_n \to 0$.

The encoding function $\phi^{(n)}$ partitions the set $\Psi_n(\eta)$ into τ_n non-intersecting subsets $\{S_i\}_{i=1}^{\tau_n}$ such that $\phi^{(n)}(\hat{x}^n) = i$ for any $\hat{x}^n \in S_i$. Define the following distribution:

$$P_{\underline{\hat{X}}^n}(\hat{x}^n) \triangleq \frac{P_{\hat{X}}^n(\hat{x}^n) \cdot \mathbb{1}\{\hat{x}^n \in \Psi_n(\eta)\}}{P_{\hat{X}}^n(\Psi_n(\eta))}. \tag{A75}$$

Please note that this distribution, henceforth denoted as $P^{(n)}$, corresponds to a uniform distribution over $\Psi_n(\eta)$ because all sequences in $\Psi_n(\eta)$ have the same type $\tilde{P}_{\hat{X}}$, and the probability is uniform on a type class under any i.i.d. measure.

Finally, define the following truncated joint distribution:

$$rClP_{\underline{MX}^n\underline{\hat{X}}^n\underline{Y}^n}(m, x^n, \hat{x}^n, y^n) \triangleq \mathbb{1}\left\{\phi^{(n)}(x^n) = m\right\} P_{X|\hat{X}}^n(x^n|\hat{x}^n) P_{\underline{\hat{X}}^n}(\hat{x}^n) P_{Y|X}^n(y^n|x^n). \tag{A76}$$

(2) *Analysis of Type-II Error Exponent:*

The proof of the upper bound on the error exponent relies on the following Lemma A1. For a set $A \subseteq \hat{\mathcal{X}}^n$, let $\mathcal{B}(A, \eta)$ denote the collection of all η-images of A, define $Q_{X\hat{X}Y} \triangleq P_{\hat{X}|X} Q_{XY}$ and

$$\kappa_{V^n}(A, Q_{\hat{X}Y}, \eta) \triangleq \frac{\min_{B \in \mathcal{B}(A,\eta)} Q_{\hat{X}Y}^n(A \times B)}{P_{\hat{X}}^n(A)}. \tag{A77}$$

This quantity is a generalization of the minimum cardinality of the η-images in [38] and is closely related to the minimum type-II error probability associated with the set A.

For the testing against independence setup, $Q_{\hat{X}Y} = P_{\hat{X}} \cdot P_Y$, and thus

$$\frac{Q_{\hat{X}Y}^n(A \times B)}{P_{\hat{X}}^n(A)} = \frac{P_{\hat{X}}^n(A) P_Y^n(B)}{P_{\hat{X}}^n(A)} = P_Y^n(B), \tag{A78}$$

and $\kappa_{V^n}(A, Q_{\hat{X}Y}, \eta)$ is simply written as $\kappa_{V^n}(A, \eta)$ and is given by

$$\kappa_{V^n}(A, \eta) \triangleq \min_{B \in \mathcal{B}(A,\eta)} P_Y^n(B). \tag{A79}$$

Lemma A1 (Lemma 3 in [4]). *For any set $A \subseteq \hat{\mathcal{X}}^n$, consider a distribution $P_A^{(n)}$ over A and let $P_A^{(n)} V^n$ be its corresponding output distribution induced by the channel V^n, i.e.,*

$$P_A^{(n)} V^n(y^n) \triangleq \sum_{\hat{x}^n \in A} P_A^{(n)}(\hat{x}^n) V^n(y^n|\hat{x}^n). \tag{A80}$$

Then, for every $\delta' > 0$, $0 < \eta < 1$, we have

$$\kappa_{V^n}(A, \eta) \geq 2^{-D(P_A^{(n)} V^n \| P_Y^n) - n\delta'} \tag{A81}$$

for sufficiently large n.

Let $P_i^{(n)} V^n$ be the distribution of the random variable $\underline{Y}^n$ given $\underline{M} = i$. The type-II error probability can be lower-bounded as:

$$\begin{aligned}
\beta_n &\geq \sum_{\hat{x}^n \in \Psi_n(\eta)} P_{\hat{X}}^n(\hat{x}^n) \cdot P_Y^n\left(D_{\phi^{(n)}(\hat{x}^n)}\right) && \text{(A82)}\\
&= \sum_{i=1}^{\tau_n} P_{\hat{X}}^n(S_i) \cdot P_Y^n(D_i) && \text{(A83)}\\
&\geq \sum_{i=1}^{\tau_n} P_{\hat{X}}^n(S_i) \cdot \kappa_{V^n}(S_i, \eta) && \text{(A84)}\\
&= P_{\hat{X}}^n(\Psi_n(\eta)) \cdot \sum_{i=1}^{\tau_n} P^{(n)}(S_i) \cdot \kappa_{V^n}(S_i, \eta) && \text{(A85)}\\
&\geq 2^{-n\delta'} \cdot P_{\hat{X}}^n(\Psi_n(\eta)) \cdot \sum_{i=1}^{\tau_n} P^{(n)}(S_i) \cdot 2^{-D\left(P_i^{(n)} V^n \middle\| P_Y^n\right)} && \text{(A86)}\\
&\geq 2^{-n\delta'} \cdot P_{\hat{X}}^n(\Psi_n(\eta)) \cdot 2^{-\sum_{i=1}^{\tau_n} P^{(n)}(S_i) \cdot D\left(P_i^{(n)} V^n \middle\| P_Y^n\right)} && \text{(A87)}\\
&\geq \frac{2^{-n\delta'}\delta}{(n+1)^{|\hat{\mathcal{X}}|}} \cdot 2^{-\sum_{i=1}^{\tau_n} P^{(n)}(S_i) \cdot D\left(P_i^{(n)} V^n \middle\| P_Y^n\right)}, && \text{(A88)}
\end{aligned}$$

where (A84) follows from the definition of $\kappa_{V^n}(S_i, \eta)$, (A86) follows because Lemma A1 implies that for any distribution $P_i^{(n)}$ over the set S_i it holds that $\kappa_{V^n}(S_i, \eta) \geq 2^{-D\left(P_i^{(n)} V^n \| P_Y^n\right) - n\delta'}$, (A87) follows because of the convexity of the function $t \mapsto 2^t$, and (A88) follows by (A70) and the fact that $\Pr(A) \geq \Pr(A \cap B)$. Hence,

$$-\frac{1}{n} \log \beta_n - \delta'' \leq \frac{1}{n} \sum_{i=1}^{\tau_n} P^{(n)}(S_i) \cdot D\left(P_i^{(n)} V^n \| P_Y^n\right), \tag{A89}$$

where $\delta'' \triangleq \delta' - \frac{1}{n} \log \frac{\delta}{(n+1)^{|\hat{\mathcal{X}}|}}$.

(3) *Single-letterization Steps and Analyses of Rate and Privacy Constraints:*

In the following, we proceed to provide a single-letter characterization of the upper bound in (A89). Considering the fact that $P^{(n)}(S_i) = P_{\underline{M}}(i)$, the right-hand-side of (A89) can be upper-bounded as follows:

$$\frac{1}{n}\sum_{i=1}^{\tau_n} P^{(n)}(S_i)\cdot D(P_i^{(n)}V^n\|P_Y^n) = \frac{1}{n}\sum_{i=1}^{\tau_n}\sum_{y^n\in\mathcal{Y}^n} P_{\underline{M}\underline{Y}^n}(i,y^n)\log\frac{P_{\underline{Y}^n|\underline{M}}(y^n|i)}{P_Y^n(y^n)} \tag{A90}$$

$$= -\frac{1}{n}H(\underline{Y}^n|\underline{M}) - \frac{1}{n}\sum_{y^n\in\mathcal{Y}^n} P_{\underline{Y}^n}(y^n)\log P_Y^n(y^n) \tag{A91}$$

$$= -\frac{1}{n}H(\underline{Y}^n|\underline{M}) - \frac{1}{n}\sum_{y^n\in\mathcal{Y}^n} P_{\underline{Y}^n}(y^n)\sum_{t=1}^{n}\log P_Y(y_t) \tag{A92}$$

$$= -\frac{1}{n}H(\underline{Y}^n|\underline{M}) - \frac{1}{n}\sum_{t=1}^{n}\sum_{y^n\in\mathcal{Y}^n} P_{\underline{Y}^n}(y^n)\log P_Y(y_t) \tag{A93}$$

$$= -\frac{1}{n}H(\underline{Y}^n|\underline{M}) - \frac{1}{n}\sum_{t=1}^{n}\sum_{y_t\in\mathcal{Y}} P_{\underline{Y}_t}(y_t)\log P_Y(y_t) \tag{A94}$$

$$= -\frac{1}{n}H(\underline{Y}^n|\underline{M}) + \frac{1}{n}\sum_{t=1}^{n}\left[H(\underline{Y}_t) + D(P_{\underline{Y}_t}\|P_Y)\right] \tag{A95}$$

$$= \frac{1}{n}\sum_{t=1}^{n}\left[H(\underline{Y}_t) - H(\underline{Y}_t|\underline{M},\underline{Y}^{t-1}) + D(P_{\underline{Y}_t}\|P_Y)\right] \tag{A96}$$

$$\le \frac{1}{n}\sum_{t=1}^{n} I(\underline{M},\underline{X}^{t-1},\underline{\hat{X}}^{t-1};\underline{Y}_t) + \frac{1}{n}\sum_{t=1}^{n} D(P_{\underline{Y}_t}\|P_Y) \tag{A97}$$

$$= \frac{1}{n}\sum_{t=1}^{n} I(\underline{U}_t;\underline{Y}_t) + \frac{1}{n}\sum_{t=1}^{n} D(P_{\underline{Y}_t}\|P_Y) \tag{A98}$$

$$= I(\underline{U};\underline{Y}) + D(P_{\underline{Y}}\|P_Y). \tag{A99}$$

Here, (A96)–(A99) are justified in the following:

- (A96) follows by the chain rule;
- (A97) follows from the Markov chain $\underline{Y}^{t-1} \to (\underline{M},\underline{X}^{t-1},\underline{\hat{X}}^{t-1}) \to \underline{Y}_t$;
- (A98) follows from the definition

$$\underline{U}_t \triangleq (\underline{M},\underline{X}^{t-1},\underline{\hat{X}}^{t-1}); \tag{A100}$$

- (A99) follows by defining a time-sharing random variable T over $\{1,\ldots,n\}$ and the following

$$\underline{U} \triangleq (\underline{U}_T, T), \qquad \underline{Y} \triangleq \underline{Y}_T. \tag{A101}$$

This leads to the following upper-bound on the type-II error exponent:

$$-\frac{1}{n}\log\beta_n \le I(\underline{U};\underline{Y}) + D(P_{\underline{Y}}\|P_Y) + \delta''. \tag{A102}$$

Next, the rate constraint satisfies the following:

$$nR \ge H(\underline{M}) \tag{A103}$$

$$\ge I(\underline{M};\underline{\hat{X}}^n) \tag{A104}$$

$$= H(\underline{\hat{X}}^n) - H(\underline{\hat{X}}^n|\underline{M}) \tag{A105}$$

$$= \log\left|\Psi_n(\eta)\right| - H(\underline{\hat{X}}^n|\underline{M}) \tag{A106}$$

$$\ge n(H(\hat{X}) - \delta_2) - H(\underline{\hat{X}}^n|\underline{M}) \tag{A107}$$

$$= nH(\hat{X}) - \sum_{t=1}^{n} H(\underline{\hat{X}}_t|\underline{\hat{X}}^{t-1}, \underline{M}) - n\delta_2 \tag{A108}$$

$$= nH(\hat{X}) - \sum_{t=1}^{n} H(\underline{\hat{X}}_t|\underline{U}_t) - n\delta_2 \tag{A109}$$

$$= nH(\hat{X}) - nH(\underline{\hat{X}}|\underline{U}) - n\delta_2 \tag{A110}$$

where (A106) follows because the distribution $P_{\underline{\hat{X}}^n}$ is uniform over the set $\Psi_n(\eta)$; (A107) follows from (A74); (A109) follows from the definition in (A100); (A110) follows by defining $\underline{\hat{X}} \triangleq \underline{\hat{X}}_T$.

Finally, the privacy measure satisfies the following:

$$nL \geq I(X^n; \hat{X}^n) \tag{A111}$$

$$\geq I(\underline{X}^n; \underline{\hat{X}}^n) \tag{A112}$$

$$= H(\underline{\hat{X}}^n) - H(\underline{\hat{X}}^n|\underline{X}^n) \tag{A113}$$

$$= \log\left|\Psi_n(\eta)\right| - H(\underline{\hat{X}}^n|\underline{X}^n) \tag{A114}$$

$$= n\left(H(\hat{X}) - \delta_2\right) - H(\underline{\hat{X}}^n|\underline{X}^n) \tag{A115}$$

$$= n\left(H(\hat{X}) - \delta_2\right) - \sum_{t=1}^{n} H(\underline{\hat{X}}_t|\underline{\hat{X}}^{t-1}, \underline{X}^n) \tag{A116}$$

$$\geq n\left(H(\hat{X}) - \delta_2\right) - \sum_{t=1}^{n} H(\underline{\hat{X}}_t|\underline{X}_t) \tag{A117}$$

$$= nH(\hat{X}) - nH(\underline{\hat{X}}|\underline{X}) - n\delta_2, \tag{A118}$$

where (A112) follows because $(\underline{X}^n, \underline{\hat{X}}^n)$ are functions of $(X^n, \hat{X}^n)$ and from data processing inequality, (A114) follows because $P_{\underline{\hat{X}}^n}$ is uniform over the set $\Psi_n(\eta)$ (see definition in (A75)), (A115) follows from (A74), and (A118) follows by defining $\underline{X} \triangleq (\underline{X}_T, T)$, $\underline{\hat{X}} \triangleq (\underline{\hat{X}}_T, T)$ and choosing T uniformly over $\{1, \ldots, n\}$.

Since $\Psi_n(\eta) \subseteq \mathcal{T}^n(\tilde{P}_{\hat{X}})$, for any $\hat{x} \in \hat{\mathcal{X}}$,

$$P_{\underline{\hat{X}}}(\hat{x}) = \frac{1}{n}\sum_{t=1}^{n} P_{\underline{\hat{X}}_t}(\hat{x}) \tag{A119}$$

$$= \sum_{\hat{x}^n \in \Psi_n(\eta)} \frac{N\left(\hat{x}|\hat{x}^n\right)}{n \cdot |\Psi_n(\eta)|} \tag{A120}$$

$$= \tilde{P}_{\hat{X}}(\hat{x}). \tag{A121}$$

Recall that $|\tilde{P}_{\hat{X}} - P_{\hat{X}}| \leq \mu_n$ with $\mu_n = n^{-1/3}$. Hence, from (A121), it holds that $|P_{\underline{\hat{X}}} - P_{\hat{X}}| \leq \mu_n$. By the definitions of $\underline{\hat{X}}$, $\underline{X}$ and $\underline{Y}$, we have $P_{\hat{X}|X} = P_{\underline{\hat{X}}|\underline{X}}$ and $P_{Y|X} = P_{\underline{Y}|\underline{X}} = V$. The random variable U is chosen over the same alphabet as $\underline{U}$ and such that $P_{U|\hat{X}} = P_{\underline{U}|\underline{\hat{X}}}$.

Since $P_Y(y) > 0$ for all $y \in \mathcal{Y}$, letting $n \to \infty$ and $\mu_n \to 0$ and the uniform continuity of the involved information-theoretic quantities yields the following upper bound on the optimal error exponent:

$$rCl\theta_\epsilon^*(R, L) \leq I(U; Y), \tag{A122}$$

subject to the rate constraint:

$$rClR \geq I(U; \hat{X}), \tag{A123}$$

and the privacy constraint:

$$rClL \geq \qquad\qquad I(X; \hat{X}). \tag{A124}$$

This concludes the proof of converse.

Appendix C. Proof of Converse of Proposition 1

We simplify Theorem 2 for the proposed binary setup. As discussed in Section 4.3, from the fact that $|\hat{\mathcal{X}}| = 2$ and the symmetry of the source X on its alphabet, without loss of optimality, we can choose $P_{\hat{X}|X}$ to be a BSC. First, consider the rate constraint:

$$\begin{aligned} R &\geq I(U;\hat{X}) && \text{(A125)}\\ &= H(\hat{X}) - H(\hat{X}|U) && \text{(A126)}\\ &= 1 - H(\hat{X}|U), && \text{(A127)} \end{aligned}$$

which can be equivalently written as the following:

$$H(\hat{X}|U) \geq 1 - R. \tag{A128}$$

Also, the privacy criterion can be simplified as follows:

$$\begin{aligned} L &\geq I(\hat{X};X) && \text{(A129)}\\ &= H(\hat{X}) - H(\hat{X}|X) && \text{(A130)}\\ &= 1 - H(\hat{X}|X) && \text{(A131)}\\ &= 1 - H(\hat{Z}), && \text{(A132)} \end{aligned}$$

which can be equivalently written as

$$H(\hat{Z}) \geq 1 - L. \tag{A133}$$

Now, consider the error exponent θ as follows:

$$\begin{aligned} \theta &\leq I(U;Y) && \text{(A134)}\\ &= H(Y) - H(Y|U) && \text{(A135)}\\ &= H(Y) - H(X \oplus N|U) && \text{(A136)}\\ &= H(Y) - H(\hat{X} \oplus \hat{Z} \oplus N|U) && \text{(A137)}\\ &\leq H(Y) - h_{\mathrm{b}}\left(h_{\mathrm{b}}^{-1}(H(\hat{X}|U)) \star h_{\mathrm{b}}^{-1}(1-L) \star q\right) && \text{(A138)}\\ &\leq H(Y) - h_{\mathrm{b}}\left(h_{\mathrm{b}}^{-1}(1-R) \star h_{\mathrm{b}}^{-1}(1-L) \star q\right), && \text{(A139)} \end{aligned}$$

where (A138) follows from Mrs. Gerber's lemma [39] (Theorem 1) and the fact that $(\hat{Z}, N)$ is independent of U and also from (A133); (A139) follows from (A128). This concludes the proof of the proposition.

Appendix D. Euclidean Approximation of Testing agianst Independence

We analyze the Euclidean approximation with the parameters, $\mathbf{W}$, $\psi_u(\hat{x})$, $\phi_{\hat{x}}(x)$ and $\Lambda_u(x)$ defined in Section 4.4. Notice that since $U \to \hat{X} \to X \to Y$ forms a Markov chain, it holds that, for any $u \in \mathcal{U}$,

$$\mathbf{P}_{Y|U=u} = \mathbf{W}\mathbf{P}_{X|U=u}. \tag{A140}$$

Now, consider the following chain of equalities for any $x \in \mathcal{X}$:

$$P_{X|U}(x|u) = \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{X\hat{X}|U}(x,\hat{x}|u) \tag{A141}$$

$$= \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}|U}(\hat{x}|u)\; P_{X|\hat{X},U}(x|\hat{x},u) \tag{A142}$$

$$= \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}|U}(\hat{x}|u)\; P_{X|\hat{X}}(x|\hat{x}) \tag{A143}$$

$$= \sum_{\hat{x}\in\hat{\mathcal{X}}} \left(P_{\hat{X}}(\hat{x}) + \psi_u(\hat{x})\right)\; \left(P_X(x) + \phi_{\hat{x}}(x)\right) \tag{A144}$$

$$= P_X(x) + \sum_{\hat{x}\in\hat{\mathcal{X}}} \psi_u(\hat{x})\; \phi_{\hat{x}}(x) + \sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}}(\hat{x})\; \phi_{\hat{x}}(x) + P_X(x) \sum_{\hat{x}\in\hat{\mathcal{X}}} \psi_u(\hat{x}) \tag{A145}$$

$$= P_X(x) + \sum_{\hat{x}\in\hat{\mathcal{X}}} \psi_u(\hat{x})\; \phi_{\hat{x}}(x), \tag{A146}$$

where (A143)—(A146) are justified in the following:

- (A143) follows from the Markov chain $U \to \hat{X} \to X$ where given $\hat{X}$, U and X are independent;
- (A144) follows from (30) and (36);
- (A146) follows from (31) and also from (36) which yields the following:

$$\sum_{\hat{x}\in\hat{\mathcal{X}}} P_{\hat{X}}(\hat{x}) \cdot \phi_{\hat{x}}(x) = 0. \tag{A147}$$

With the definition of $\Lambda_u(x)$ in (42), we can write

$$P_{X|U}(x|u) = P_X(x) + \Lambda_u(x), \qquad \forall x \in \mathcal{X}, u \in \mathcal{U}. \tag{A148}$$

Thus, we get

$$\mathbf{P}_{Y|U=u} = \mathbf{W}\mathbf{P}_X + \mathbf{W}\mathbf{\Lambda}_u \tag{A149}$$

$$= \mathbf{P}_Y + \mathbf{W}\mathbf{\Lambda}_u. \tag{A150}$$

Applying the χ^2-approximation and using (A150), we can rewrite $I(U;Y)$ as follows:

$$I(U;Y) \approx \frac{1}{2}\; \log e \sum_{u\in\mathcal{U}} P_U(u)\; \left\| \left[\sqrt{P_Y}\right]^{-1} \mathbf{W}\mathbf{\Lambda}_u \right\|^2 \tag{A151}$$

The above approximation with the definition of the vector $\mathbf{\Lambda}_u$ in (43) yields the optimization problem in (45).

Appendix E. Proof of Proposition 2

Achievability: We specialize the achievable scheme of Theorem 2 to the proposed Gaussian setup. We choose the auxiliary random variables as in (63) and (65). Notice that from the Markov chain $U \to \hat{X} \to X \to Y$ and also the Gaussian choice of $\hat{X}$ in (63) which was discussed in Section 4.5, we can write $Y = \rho\hat{X} + F$ where $F \sim \mathcal{N}\left(0, 1 - \rho^2 \cdot (1 - 2^{-2L})\right)$ is independent of $\hat{X}$. These choices of auxiliary random variables lead to the following rate constraint:

$$R \geq \frac{1}{2} \log\left(\frac{1 - 2^{-2L}}{\beta^2}\right), \tag{A152}$$

which can be equivalently written as:

$$2^{-2R} \cdot \left(1 - 2^{-2L}\right) \leq \beta^2. \tag{A153}$$

The optimal error exponent is also lower bounded as follows

$$\theta_\epsilon^*(R,L) \geq \frac{1}{2}\log\left(\frac{1}{1-\rho^2\cdot(1-2^{-2L}-\beta^2)}\right). \tag{A154}$$

Combining (A153) and (A154) gives the lower bound on the error exponent in (64).
Converse: Consider the following upper bound on the optimal error exponent in Theorem 2:

$$\begin{aligned}
\theta_\epsilon^*(R,L) &\leq I(U;Y) && \text{(A155)}\\
&= h(Y) - h(Y|U) && \text{(A156)}\\
&= \frac{1}{2}\log(2\pi e) - h(Y|U) && \text{(A157)}\\
&= \frac{1}{2}\log(2\pi e) - h\big(\rho\hat{X}+F\big|U\big) && \text{(A158)}\\
&\leq \frac{1}{2}\log(2\pi e) - \frac{1}{2}\log\left(2^{2h(\rho\hat{X}|U)} + 2\pi e\left(1-\rho^2\cdot(1-2^{-2L})\right)\right) && \text{(A159)}\\
&\leq \frac{1}{2}\log(2\pi e) - \frac{1}{2}\log\left(\rho^2\,2^{2h(\hat{X}|U)} + 2\pi e\left(1-\rho^2\cdot(1-2^{-2L})\right)\right), && \text{(A160)}
\end{aligned}$$

where (A159) follows from the entropy power inequality (EPI) [34] (Chapter 2). Now, consider the rate constraint as follows:

$$\begin{aligned}
R &\geq I(\hat{X};U) && \text{(A161)}\\
&= h(\hat{X}) - h(\hat{X}|U) && \text{(A162)}\\
&= \frac{1}{2}\log\left(2\pi e\left(1-2^{-2L}\right)\right) - h(\hat{X}|U), && \text{(A163)}
\end{aligned}$$

which is equivalent to

$$2^{2h(\hat{X}|U)} \geq 2\pi e\cdot 2^{-2R}\cdot\left(1-2^{-2L}\right). \tag{A164}$$

Considering (A160) with (A164) yields the following upper bound on the error exponent:

$$\begin{aligned}
\theta_\epsilon^*(R,L) &\leq \frac{1}{2}\log(2\pi e) - \frac{1}{2}\log\left(2\pi e\rho^2 2^{-2R}\left(1-2^{-2L}\right) + 2\pi e\left(1-\rho^2\,(1-2^{-2L})\right)\right) && \text{(A165)}\\
&= \frac{1}{2}\log\left(\frac{1}{1-\rho^2\,(1-2^{-2R})\,(1-2^{-2L})}\right). && \text{(A166)}
\end{aligned}$$

This concludes the proof of the proposition.

References

1. Ahlswede, R.; Csiszàr, I. Hypothesis testing with communication constraints. *IEEE Trans. Inf. Theory* **1986**, *32*, 533–542. [CrossRef]
2. Zhao, W.; Lai, L. Distributed testing against independence with multiple terminals. In Proceedings of the 2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 30 September–3 October 2014; pp. 1246–1251.
3. Xiang, Y.; Kim, Y.H. Interactive hypothesis testing against independence. In Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, 7–12 July 2013; pp. 2840–2844.
4. Tian, C.; Chen, J. Successive refinement for hypothesis testing and lossless one-helper problem. *IEEE Trans. Inf. Theory* **2008**, *54*, 4666–4681. [CrossRef]
5. Rahman, M.S.; Wagner, A.B. On the optimality of binning for distributed hypothesis testing. *IEEE Trans. Inf. Theory* **2012**, *58*, 6282–6303. [CrossRef]

6. Sreekuma, S.; Gündüz, D. Distributed Hypothesis Testing Over Noisy Channels. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017.
7. Salehkalaibar, S.; Wigger, M.; Timo, R. On hypothesis testing against independence with multiple decision centers. *arXiv* **2017**, arXiv:1708.03941.
8. Salehkalaibar, S.; Wigger, M.; Wang, L. Hypothesis Testing In Multi-Hop Networks. *arXiv* **2017**, arXiv:1708.05198.
9. Mhanna, M.; Piantanida, P. On secure distributed hypothesis testing. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, China, 14–19 June 2015; pp. 1605–1609.
10. Han, T.S. Hypothesis testing with multiterminal data compression. *IEEE Trans. Inf. Theory* **1987**, *33*, 759–772. [CrossRef]
11. Shimokawa, H.; Han, T.; Amari, S.I. Error bound for hypothesis testing with data compression. *IEEE Trans. Inf. Theory* **1994**, *32*, 533–542.
12. Ugur, Y.; Aguerri, I.E.; Zaidi, A. Vector Gaussian CEO Problem Under Logarithmic Loss and Applications. *arXiv* **2018**, arXiv:1811.03933.
13. Zaidi, A.; Aguerri, I.E.; Caire, G.; Shamai, S. Uplink oblivious cloud radio access networks: An information theoretic overview. In Proceedings of the 2018 Information Theory and Applications Workshop (ITA), San Diego, CA, USA, 11–16 February 2018.
14. Aguerri, I.E.; Zaidi, A.; Caire, G.; Shamai, S. On the capacity of cloud radio access networks with oblivious relaying. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017.
15. Aguerri, I.E.; Zaidi, A. Distributed information bottleneck method for discrete and Gaussian sources. In Proceedings of the 2018 International Zurich Seminar on Information and Communication (IZS), Zurich, Switzerland, 21–23 February 2018.
16. Aguerri, I.E.; Zaidi, A. Distributed variational representation learning. *arXiv* **2018**, arXiv:1807.04193.
17. Evfimievski, A.V.; Gehrke, J.; Srikant, R. Limiting privacy breaches in privacy preserving data mining. In Proceedings of the Twenty-Second Symposium on Principles of Database Systems, San Diego, CA, USA, 9–11 June 2003; pp. 211–222.
18. Smith, G. On the Foundations of Quantitative Information Flow. In *Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures: Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2009*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 288–302.
19. Sankar, L.; Rajagopalan, S.R.; Poor, H.V. Utility-Privacy Tradeoffs in Databases: An Information-Theoretic Approach. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 838–852. [CrossRef]
20. Liao, J.; Sankar, L.; Tan, V.Y.F.; Calmon, F. Hypothesis Testing Under Mutual Information Privacy Constraints in the High Privacy Regime. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1058–1071. [CrossRef]
21. Barthe, G.; Köpf, B. Information-theoretic bounds for differentially private mechanisms. In Proceedings of the 2011 IEEE 24th Computer Security Foundations Symposium, Cernay-la-Ville, France, 27–29 June 2011; pp. 191–204.
22. Issa, I.; Wagner, A.B. Operational definitions for some common information leakage metrics. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 769–773.
23. Liao, J.; Sankar, L.; Calmon, F.; Tan, V.Y.F. Hypothesis testing under maximal leakage privacy constraints. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 779–783.
24. Wagner, I.; Eckhoff, D. Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv. (CSUR)* **2018**, *51*, to appear. [CrossRef]
25. Dwork, C. Differential Privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, Part II (ICALP 2006)*; Springer: Venice, Italy, 2006; Volume 4052, pp. 1–12.
26. Dwork, C.; Kenthapadi, K.; McSherry, F.; Mironov, I.; Naor, M. Our Data, Ourselves: Privacy Via Distributed Noise Generation. In *Advances in Cryptology (EUROCRYPT 2006)*; Springer: Saint Petersburg, Russia, 2006; Volume 4004, pp. 486–503.
27. Dwork, C. *Differential Privacy: A Survey of Results*; Chapter Theory and Applications of Models of Computation; TAMC 2008; Lecture Notes in Computer Science; Springer: Heidelberg, Germany, 2008; Volume 4978.

28. Wasserman, L.; Zhou, S. A statistical framework for differential privacy. *J. Am. Stat. Assoc.* **2010**, *105*, 375–389. [CrossRef]
29. Sreekumar, A.C.; Gunduz, D. Distributed hypothesis testing with a privacy constraint. *arXiv* **2018**, arXiv:1806.02015.
30. Borade, S.; Zheng, L. Euclidean Information Theory. In Proceedings of the 2008 IEEE International Zurich Seminar on Communications, Zurich, Switzerland, 12–14 March 2008; pp. 14–17.
31. Huang, S.; Suh, C.; Zheng, L. Euclidean information theory of networks. *IEEE Trans. Inf. Theory* **2015**, *61*, 6795–6814. [CrossRef]
32. Viterbi, A.J.; Omura, J.K. *Principles of Digital Communication and Coding*; McGraw-Hill: New York, NY, USA, 1979.
33. Weinberger, N.; Merhav, N. Optimum tradeoffs between the error exponent and the excess-rate exponent of variable rate Slepian-Wolf coding. *IEEE Trans. Inf. Theory* **2015**, *61*, 2165–2190. [CrossRef]
34. El Gamal, A.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011.
35. Shalaby, H.M.H.; Papamarcou, A. Multiterminal detection with zero-rate data compression. *IEEE Trans. Inf. Theory* **1992**, *38*, 254–267. [CrossRef]
36. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; Wiley: Hoboken, NJ, USA, 2006.
37. Watanabe, S. Neyman-Pearson Test for Zero-Rate Multiterminal Hypothesis Testing. *IEEE Trans. Inf. Theory* **2018**, *64*, 4923–4939. [CrossRef]
38. Csiszàr, I.; Körner, J. *Information theory: Coding Theorems for Discrete Memoryless Systems*; Academic Press: New York, NY, USA, 1982.
39. Wyner, A.D.; Ziv, J. A theorem on the entropy of certain binary sequences and applications (Part I). *IEEE Trans. Inf. Theory* **1973**, *19*, 769–772. [CrossRef]