Unifying Privacy Measures via Maximal (α, β)-Leakage (MαbeL)

Atefeh Gilani, *Student Member, IEEE*, Gowtham R. Kurri, *Member, IEEE*, Oliver Kosut, *Senior Member, IEEE*, and Lalitha Sankar, *Senior Member, IEEE*

***Abstract*— We introduce a family of information leakage measures called *maximal* (α, β)*-leakage* (MαbeL), parameterized by real numbers α and β greater than or equal to 1. The measure is formalized via an operational definition involving an adversary guessing an unknown (randomized) function of the data given the released data. We obtain a simplified computable expression for the measure and show that it satisfies several basic properties such as monotonicity in β for a fixed α, non-negativity, data processing inequalities, and additivity over independent releases. We highlight the relevance of this family by showing that it bridges several known leakage measures, including maximal α-leakage ($\beta = 1$), maximal leakage ($\alpha = \infty, \beta = 1$), local differential privacy (LDP) ($\alpha = \infty, \beta = \infty$), and local Rényi differential privacy (LRDP) ($\alpha = \beta$), thereby giving an operational interpretation to local Rényi differential privacy. We also study a conditional version of MαbeL on leveraging which we recover differential privacy and Rényi differential privacy. A new variant of LRDP, which we call *maximal Rényi leakage*, appears as a special case of MαbeL for $\alpha = \infty$ that smoothly tunes between maximal leakage ($\beta = 1$) and LDP ($\beta = \infty$). Finally, we show that a vector form of the maximal Rényi leakage relaxes differential privacy under Gaussian and Laplacian mechanisms.**

***Index Terms*— Maximal leakage, maximal α-leakage, (local) differential privacy, (local) Rényi differential privacy, Shannon channel capacity.**

I. Introduction

How much information does an observation released to an adversary reveal/leak about correlated sensitive data? This fundamental question arises in many privacy problems whenever data about users is stored (e.g., social networks and cloud-based services) and a certain level of information leakage is unavoidable in exchange for certain services. Limiting such an information leakage is desirable. Quantifying such leakage is the first step towards limiting it. In an effort to quantify this leakage precisely, a variety of privacy measures have been proposed in computer science [2], [3], [4], [5], [6], [7], [8] and in information theory [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20].

For any leakage measure, one of the key challenges is to associate an operational interpretation to it, so that a certain amount of leakage corresponds to a particular privacy guarantee. Only a few leakage measures possess such an operational meaning. For example, the works in [16] and [17], which pertain to the release of observation due to a side channel, measure privacy in terms of an adversary's gain in *guessing* the sensitive data after observing the released data. In particular, Issa et al. [16] consider an adversary interested in guessing a possibly randomized function of X. They study the logarithm of the multiplicative increase, upon observing Y, of the probability of correctly guessing a randomized function of X, say U, maximized over all the random variables U such that $U - X - Y$ forms a Markov chain. This maximization captures the scenario that the function of interest U is unknown to the system designer. The resulting quantity is referred to as *maximal leakage* (MaxL). Liao et al. [17] later generalized maximal leakage to a family of leakages, *maximal α-leakage* (Max-αL) that consider a family of losses, namely α-loss, to quantify the adversarial gain. Thus, similar to MaxL, Max-αL quantifies the maximal logarithmic gain in a monotonically increasing power function (dependent on α) applied to the probability of correctly guessing. By doing so, [17] presents an operational interpretation of leakage measures using adversarial loss functions.

Among leakage measures motivated by worst-case adversaries, *differential privacy* (DP) [2] has emerged as the gold standard. Relegating precise definitions to the sequel, we state that a differentially private algorithm guarantees that its outputs restrict the adversary from distinguishing between neighboring datasets (i.e., the datasets that differ only in a single data entry), where each dataset can be viewed as n instantiations of X. An operational interpretation of DP in the framework of hypothesis testing is given by Kairouz et al. [21], where they show that it determines the trade-off between probabilities of false alarm and missed detection. When privacy guarantees have to be provided in a distributed setting, *local*

Manuscript received 5 April 2023; revised 21 November 2023; accepted 17 March 2024. Date of publication 3 April 2024; date of current version 21 May 2024. This work was supported in part by NSF under Grant CIF-1901243, Grant CIF-2312666, and Grant CIF-2007688. An earlier version of this paper was presented in part at the 2022 Information Theory Workshop (ITW) [DOI: 10.1109/ITW54588.2022.9965918]. *(Corresponding author: Atefeh Gilani.)*

Atefeh Gilani, Oliver Kosut, and Lalitha Sankar are with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85281 USA (e-mail: agilani2@asu.edu; okosut@asu.edu; lalithasankar@asu.edu).

Gowtham R. Kurri was with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85281 USA. He is now with the Signal Processing and Communications Research Centre, International Institute of Information Technology, Hyderabad, Telangana 500032, India (e-mail: gowtham.kurri@iiit.ac.in).

Communicated by A. Ozgur, Associate Editor for Security and Privacy.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2024.3384922.

Digital Object Identifier 10.1109/TIT.2024.3384922

0018-9448 © 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

differential privacy (LDP) [5], [6] provides strong privacy guarantees between any two realizations of X. Issa et al. [16] extended their definition of maximal leakage to introduce a *worst-case* measure via *maximal realizable leakage* (MaxRL) by taking a maximum over all realizations of Y. They show that maximizing MaxRL over all the distributions P_X yields LDP, thereby providing an operational interpretation to the latter. In the context of composing DP outputs sequentially, *Rényi differential privacy* (RDP) [15] has emerged as a better variant to compute tight DP guarantees over multiple compositions of differentially private algorithms. Specifically, RDP relaxes DP based on the Rényi divergence [22]. One can define *local Rényi differential privacy* (LRDP) as a generalization of LDP based on the Rényi divergence. All the aforementioned leakage measures find applications in many areas such as privacy utility trade-offs [17], [23], [24], hypothesis testing [25], source coding [26], Census data [27], anomaly detection [28], age of information [29], membership inference [19], deep learning [30], posterior sampling [31], and mechanism design [32].

No single measure of privacy/information leakage suits all the scenarios in practice. In spite of the existence of a large number of privacy measures in the literature, it is often challenging to make an informed choice of a measure for a particular application in view of the diversity and complexity of various privacy measures. This compels a need for a unification of privacy leakage measures, in general, via a principled approach. In this paper, motivated by [16] and [17], we propose a family of information leakage measures, called *maximal* (α, β)*-leakage* (MαbeL), unifying all the aforementioned leakage measures into a structured landscape of leakage measures in an operationally motivated manner.

A. Main Contributions

The main contributions of this paper are as follows.

- We introduce MαbeL in the framework of a guessing adversary, which is parameterized by two real numbers $\alpha \in [1, \infty]$ and $\beta \in [1, \infty]$(Definition 9), and obtain a simplified computable expression for it (Theorem 1) [1]. We prove that it satisfies all the axiomatic properties of a measure of information leakage, including non-negativity, monotonicity in β for a fixed α, data-processing inequalities, and additivity over independent releases (Theorem 2) [1]. We also show that it is continuous at $(\alpha, \beta) \in [1, \infty] \times [1, \infty]$, with the exception of $\alpha = \beta = 1$ (Theorem 6).
- We show that this family of measures encompasses a host of existing leakage measures: in particular, Max-αL ($\beta = 1$), MaxL ($\alpha \to \infty, \beta = 1$), LDP ($\alpha \to \infty, \beta \to \infty$), LRDP ($\alpha = \beta$) (Proposition 1 and Figure 1a) [1]. Theorem 2 gives another proof that LDP satisfies both the post-processing and linkage inequalities[1] unlike DP which does not satisfy the linkage inequality [33]. Interestingly, MαbeL is defined apparently in terms of average-case analysis (in the spirit of MaxL and Max-αL), and yet, it recovers the worst-case LDP and LRDP by exploiting the interplay between the parameters α and β.
- We propose *conditional* MαbeL which takes into account the side-information an adversary may have and obtain a simplified computable expression for it (Theorem 3). We prove that MαbeL upper bounds conditional MαbeL if the side-information is conditionally independent of the released data given the original data (Theorem 4). That is, minimizing MαbeL is still a reasonable objective for a situation in which an adversary has access to side information which is unknown to the system designer. We also show that conditional MαbeL is subadditive over multiple releases (Theorem 5).
- We generalize the conditional MαbeL to a vector form which allows us to quantify the leakage associated with a change in only one entry of dataset with an assumption that an adversary has the knowledge of all the remaining entries (Definition 11). We show that this naturally recovers DP and RDP (Proposition 3). An important consequence of our results is an operational interpretation to RDP and LRDP. We note that this subsumes an operational meaning of LDP given by Issa et al. [16] via maximal realizable leakage.
- We introduce a reparameterization of MαbeL, called maximal (α, τ)-leakage, in terms of α and τ with $\alpha \geq 1$ and $\beta = \frac{\alpha\tau}{\alpha+\tau-1}$, where $\tau \geq 1$. We show that this new measure, in contrast to MαbeL, is monotonic in both orders (Lemma 1) and maintains continuity at all points $(\alpha, \tau) \in [1, \infty] \times [1, \infty]$ (Theorem 6). A new information-theoretic quantity arises as a special case of this leakage measure when $\alpha \to 1$. We call this measure τ*-Shannon leakage* and show that it recovers KL-divergence and Shannon channel capacity when $\tau = \infty$ and $\tau = 1$, respectively (Proposition 4 and Figure 2b).
- A new variant of LRDP, which we call *maximal Rényi leakage*, appears as a special case of MαbeL when $\alpha = \infty$ (Definition 8) that smoothly tunes between maximal leakage ($\beta = 1$) and LDP ($\beta = \infty$). Finally, we show that a vector form of maximal Rényi leakage relaxes differential privacy under Laplacian and Gaussian mechanisms (Proposition 5).

B. Related Work

There are different approaches to quantifying information leakage. The works [3], [4], and [7] quantify leakage similar to maximal leakage with an adversary interested in guessing X itself rather than its randomized functions. A variant of maximal leakage capturing the amount of information leaked about X due to disclosing a single outcome $Y = y$ rather than focusing on the *average outcome* as in maximal leakage has been studied in [20] and [34]. Several measures have been proposed to quantify information leakage, e.g., maximal correlation [35], [36], probability of correctly guessing [14], total variation distance [18], mutual information [10], [13], [37], [38], [39], [40], [41], [42].

[1] In the context of privacy, 'linkage inequality' is often used interchangeably with 'preprocessing inequality.'

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

The notion of DP is known to be very strict and has limited applicability [43], [44]. Approximate differential privacy is proposed as a relaxation of DP to allow data releases with higher utility [45]. Resorting to the fact that composition with RDP has a simple linear form compared to DP, the authors of [30] developed a method called Moments Accountant (MA) where the privacy guarantees are obtained first in terms of RDP before translating them to those of DP. The shuffle model for differential privacy, where a shuffler randomly permutes the (randomized) data of all the users before forwarding them to the (untrusted) server, is introduced in [46] and [47]. The authors of [48] and [49] obtained privacy gurantees with local randomized mechanisms for approximate DP and RDP, respectively. The role of interactivity in LDP is studied by Joseph et al. [50]. Though there has been a lot of work building up on (L)DP and (L)RDP in the literature, an operational interpretation to (L)RDP remained open so far which we settled by introducing MαbeL that subsumes (L)RDP as a special case for $\alpha = \beta$. For an extensive list of leakage measures see the surveys by Wagner and Eckhoff [51], Bloch et al. [52], and Hsu et al. [53].

C. Organization of the Paper

The remainder of this paper is organized as follows. We review various relevant information leakage measures in Section II. We introduce (conditional) MαbeL in Section III and prove that it satisfies the axiomatic properties of a leakage measure. In Section IV, we show that MαbeL recovers several existing information leakage measures as special cases. We present our results on reparameterization of MαbeL in Section V. We extend the notion of the leakage to continuous alphabets in Section VI and discuss its applications in Section VI-A.

Notation. We use capital letters to denote random variables, e.g., X, and capital calligraphic letters to denote their corresponding alphabet, e.g., $\mathcal{X}$. We write $U - X - Y$ to denote that the random variables form a Markov chain. We use $\text{supp}(X) := \{x : P_X(x) > 0\}$ to denote the support set of a discrete random variable X. We use $H(X)$, $I(X;Y)$, and $D(P_X \| Q_X)$ to denote entropy, mutual information, and relative entropy, respectively. Given two probability distributions P_X and Q_X over an alphabet $\mathcal{X}$, we write $P_X \ll Q_X$ to denote that P_X is absolutely continuous with respect to Q_X. We also consider continuous random variables and use f_X to denote the probability density function of X. We use $\log$ to denote the natural logarithm. Throughout the sequel, we use the terms *privacy mechanisms* and *conditional distributions* interchangeably. Finally, in our analyses, we employ the extended real number line, extending the real numbers to include positive and negative infinity.

II. Overview of Existing Information Leakage Measures

We review the definitions of some existing information leakage measures.

Definition 1 (Maximal leakage [16]): Let P_{XY} be a joint distribution on finite alphabet $\mathcal{X}\times\mathcal{Y}$, where X and Y represent the original data and the released data, respectively. The maximal leakage from X to Y is defined as

$$\mathcal{L}(X \to Y) := \sup_{U-X-Y} \log \frac{\max_{P_{\hat{U}|Y}} \sum_{u,y} P_{UY}(u,y) P_{\hat{U}|Y}(u|y)}{\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)}, \tag{1}$$

where U represents any randomized function of X that an adversary is interested in guessing and takes values in an arbitrary finite alphabet. Moreover, $\hat{U}$ is an estimator of U with the same support as U.

Liao et al. [17] generalized maximal leakage by introducing a tunable leakage measure known as maximal α-leakage.

Definition 2 (Maximal α-leakage [17]): Given a joint distribution P_{XY} on finite alphabet $\mathcal{X}\times\mathcal{Y}$, the maximal α-leakage from X to Y is defined as

$$\mathcal{L}_\alpha^{max}(X \to Y) := \frac{\alpha}{\alpha-1} \sup_{U-X-Y} \log \frac{\max_{P_{\hat{U}|Y}} \sum_{u,y} P_{UY}(u,y) P_{\hat{U}|Y}(u|y)^{\frac{\alpha-1}{\alpha}}}{\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)^{\frac{\alpha-1}{\alpha}}}, \tag{2}$$

for $\alpha \in (1,\infty)$ and by continuous extension of (2) for $\alpha = 1$ and $\alpha = \infty$, where U represents any randomized function of X with an arbitrary finite alphabet, and $\hat{U}$ is an estimator of U with the same support as U.

Liao et al. [17] showed that

$$\mathcal{L}_\alpha^{\max}(X \to Y) = \sup_{P_{\tilde{X}}} I_\alpha^{\mathrm{S}}(\tilde{X};Y), \tag{3}$$

where the supremum is over all the probability distributions $P_{\tilde{X}}$ on the support of P_X and $I_\alpha^{\mathrm{S}}(\cdot;\cdot)$ is the Sibson mutual information of order α [54]. Maximal α-leakage recovers Shannon channel capacity (and mutual information) and maximal leakage for $\alpha = 1$ and $\alpha = \infty$, respectively.

Conditional versions of maximal leakage and maximal α-leakage are also defined to quantify the leakage when the adversary has access to side-information [16, Definition 6], [55, Definition 3].

Definition 3 (Local differential privacy [5], [6]): Given a conditional distribution $P_{Y|X}$ with X and Y taking values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively, the local differential privacy (LDP) is defined as

$$\mathcal{L}^{LDP}(X \to Y) := \max_{\substack{y\in\mathcal{Y},\\ x,x'\in\mathcal{X}}} \log \frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')}. \tag{4}$$

Let $x^n = (x_1, x_2, \ldots, x_n)$ denote a dataset comprising n points from $\mathcal{X}$. We say $x^n = (x_1, x_2, \ldots, x_n)$ and $\tilde{x}^n = (\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n)$ are neighbouring datasets, denoted $x^n \sim \tilde{x}^n$, if the Hamming distance between them is 1, i.e., $\sum_{i=1}^n \mathbb{1}\{x_i \neq \tilde{x}_i\} = 1$, or in other words if there exists a unique $i \in [1:n]$ such that $x_i \neq \tilde{x}_i$. The following notion of differential privacy captures the privacy incurred of a user in participating in a dataset.

Definition 4 (Differential privacy [2]): Given a conditional distribution $P_{Y|X^n}$ with X^n and Y taking values in finite sets

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$\mathcal{X}^n$ and $\mathcal{Y}$, respectively, the differential privacy (DP) is defined as

$$\mathcal{L}^{DP}(X \to Y) := \max_{\substack{y \in \mathcal{Y}, x^n, \tilde{x}^n \in \mathcal{X}^n: \\ x^n \sim \tilde{x}^n}} \log \frac{P_{Y|X^n}(y|x^n)}{P_{Y|X^n}(y|\tilde{x}^n)}. \tag{5}$$

Definition 5 (Maximal realizable leakage [16]): Given a joint distribution P_{XY} on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, the maximal realizable leakage from X to Y is defined as

$$\mathcal{L}^r(X \to Y) = \sup_{U - X - Y} \log \frac{\max_y \max_u P_{U|Y}(u|y)}{\max_u P_U(u)} \tag{6}$$

where U takes values in an arbitrary finite alphabet.

In [16], it has been shown that

$$\mathcal{L}^{\text{LDP}}(X \to Y) = \sup_{P_X} \mathcal{L}^r(X \to Y), \tag{7}$$

where the supremum is over all probability distribution P_X. A natural relaxation of DP is introduced by Mironov [15] based on the Rényi divergence to allow stronger results for composition.

Definition 6 (Rényi differential privacy [15]): Given a conditional distribution $P_{Y|X^n}$ with X^n and Y taking values in finite sets $\mathcal{X}^n$ and $\mathcal{Y}$, respectively, the Rényi differential privacy (RDP) of order α is defined as

$$\begin{aligned}
&\mathcal{L}_\alpha^{RDP}(X \to Y) \\
&:= \max_{\substack{x^n, \tilde{x}^n \in \mathcal{X}^n: \\ x^n \sim \tilde{x}^n}} D_\alpha(P_{Y|X^n=x^n} \| P_{Y|X^n=\tilde{x}^n}) && (8)\\
&= \max_{\substack{x^n, \tilde{x}^n \in \mathcal{X}^n: \\ x^n \sim \tilde{x}^n}} \frac{1}{\alpha - 1} \log \sum_y P_{Y|X^n}(y|\tilde{x}^n)^{1-\alpha} P_{Y|X^n}(y|x^n)^\alpha. && (9)
\end{aligned}$$

We may define local Rényi differential privacy as a generalization of local differential privacy based on the Rényi divergence [22].

Definition 7 (Local Rényi differential privacy): Given a conditional distribution $P_{Y|X}$ with X and Y taking values in finite sets $\mathcal{X}$ and $\mathcal{Y}$, respectively, the local Rényi differential privacy (LRDP) of order α is defined as

$$\begin{aligned}
&\mathcal{L}_\alpha^{LRDP}(X \to Y) \\
&:= \max_{x, x' \in \mathcal{X}} D_\alpha(P_{Y|X=x} \| P_{Y|X=x'}) && (10)\\
&= \max_{x, x' \in \mathcal{X}} \frac{1}{\alpha - 1} \log \sum_y P_{Y|X}(y|x')^{1-\alpha} P_{Y|X}(y|x)^\alpha. && (11)
\end{aligned}$$

As $\alpha \to \infty$, it can be verified using L'Hôpital's rule that LRDP and RDP simplify to LDP and DP, respectively.

III. A Unified Measure of Information Leakage

In this section, we introduce a unified leakage measure, called maximal (α, β)-leakage (MαbeL). The new leakage measure includes maximal leakage, maximal α-leakage, local Rényi differential privacy and local differential privacy as its special cases. As our unified measure includes these leakage measures, its definition naturally inherits some complexity, mirroring that of the definitions of these existing measures. However, in Theorem 1, we shed light on its inherent complexity and significantly simplify it, thereby allowing us to relate to a large class of privacy measures. Furthermore, to recover Rényi differential privacy and differential privacy, we introduce conditional MαbeL, and provide a simplified form for it in Theorem 3.

A. MαbeL

Before introducing our most general unified leakage measure, we start with a measure which smoothly transitions between maximal leakage and LDP. The following definition makes use of the similarity between the definitions of maximal leakage and maximal realizable leakage, and the fact that the latter is related to LDP via (7).

Definition 8 (Maximal Rényi leakage of order β): Given a conditional distribution $P_{Y|X}$ (or $f_{Y|X}$) on alphabets $\mathcal{X}$ and $\mathcal{Y}$, maximal Rényi leakage of order β from X to Y for $\beta \in [1, \infty)$ is defined as

$$\mathcal{L}_\beta(X \to Y) := \sup_{P_X} \sup_{U \to X \to Y} \log \frac{\max_{P_{\hat{U}|Y}} \left[\mathbb{E}_Y \left[\left(\sum_u P_{U|Y}(u|Y) P_{\hat{U}|Y}(u|Y) \right)^\beta \right] \right]^{1/\beta}}{\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)}. \tag{12}$$

where $\hat{U}$ represents an estimator taking values from the same arbitrary finite alphabet as U. It is defined by continuous extension for $\beta \to \infty$.

There are two important aspects to this definition. First, we introduce a parameter β in the numerator in (12) thereby allowing a continuous transition from a simple average over y (at $\beta = 1$) to a maximum over y (at $\beta \to \infty$). Thus, ignoring for the moment the supremum over P_X, when $\beta \to \infty$ we recover maximal realizable leakage, and at $\beta = 1$ we recover maximal leakage. Secondly, by introducing the supremum over P_X, we do not change the value at $\beta = 1$, since maximal leakage depends on the distribution of X only through its support, and at $\beta \to \infty$ we recover LDP due to (7).

As a next step, we combine the definition of maximal Rényi leakage with that of maximal α-leakage, keeping both as special cases, and including both α and β as independent parameters. Remarkably, this yields our most general unified measure which also recovers LDP and LRDP.

Definition 9 (Maximal (α, β)-leakage (MαbeL)): Given a conditional distribution $P_{Y|X}$ (or $f_{Y|X}$) on supports $\mathcal{X}$ and $\mathcal{Y}$, the maximal (α, β)-leakage from X to Y for $(\alpha, \beta) \in (1, \infty) \times [1, \infty)$ is defined as

$$\mathcal{L}_{\alpha,\beta}(X \to Y) := \sup_{P_X} \sup_{U \to X \to Y} \frac{\alpha}{\alpha - 1} \log \frac{\max_{P_{\hat{U}|Y}} \left[\mathbb{E}_Y \left[\left(\sum_u P_{U|Y}(u|Y) P_{\hat{U}|Y}(u|Y)^{\frac{\alpha-1}{\alpha}} \right)^\beta \right] \right]^{1/\beta}}{\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)^{\frac{\alpha-1}{\alpha}}}. \tag{13}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

where $\hat{U}$ represents an estimator taking values from the same arbitrary finite alphabet as U. MαbeL is defined by its continuous extension for $(\alpha,\beta) \in \{1,\infty\} \times [1,\infty) \setminus \{(1,1)\}$ and $(\alpha,\beta) \in (1,\infty) \times \{\infty\}$. It is also defined by $\lim_{\beta\to\infty}\lim_{\alpha\to 1}\mathcal{L}_{\alpha,\beta}(X \to Y)$ and $\lim_{\beta\to\infty}\lim_{\alpha\to\infty}\mathcal{L}_{\alpha,\beta}(X \to Y)$ for $(1,\infty)$ and (∞,∞), respectively.

We remark that the definition of MαbeL in (13) recovers the definition of maximal α-leakage from (2) when $\beta = 1$. While at the outset this simplification does not appear to be the same as that of maximal α-leakage in (2) (i.e., the latter does not include a supremum over P_X), maximal α-leakage depends on the distribution of X only through its support (see (3)), and therefore, including the supremum over P_X does not change its value.

We also observe that the definition of MαbeL specializes to the definition of maximal Rényi leakage of order β in (12) for $\alpha = \infty$.

In the following theorem, we present a simplification of the expression of MαbeL in (13). As a special case of $\alpha \to \infty$, it also includes a simplified form for the maximal Rényi leakage of order β introduced in Definition 8.

Theorem 1: Let X and Y take values from finite supports $\mathcal{X}$ and $\mathcal{Y}$, respectively. For $(\alpha,\beta) \in (1,\infty) \times [1,\infty)$, M$\alpha$beL defined in (13) simplifies to

$$\mathcal{L}_{\alpha,\beta}(X \to Y) = \max_{x'\in\mathcal{X}} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_{y\in\mathcal{Y}} P_{Y|X}(y|x')^{1-\beta} \left(\sum_{x\in\mathcal{X}} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha}\right)^{\beta/\alpha}, \tag{14}$$

where $P_{\tilde{X}}$ is a probability distribution on the support of P_X. For $\alpha \to \infty$, since Definition 9 simplifies to the definition of maximal Rényi leakage of order β in (12), (14) simplifies maximal Rényi leakage of order β to

$$\mathcal{L}_{\beta}(X \to Y) = \max_{x'\in\mathcal{X}} \frac{1}{\beta} \log \sum_{y\in\mathcal{Y}} P_{Y|X}(y|x')^{1-\beta} \max_{x\in\mathcal{X}} P_{Y|X}(y|x)^{\beta}. \tag{15}$$

A detailed proof for Theorem 1 is given in Appendix A.

For $\beta \le \alpha$, the quantity inside the log in (14) is concave in $P_{\tilde{X}}$; thus the supremum over $P_{\tilde{X}}$ can be efficiently solved using convex optimization techniques. As we will show in Section IV, for $\beta \ge \alpha$, the supremum over $P_{\tilde{X}}$ can be replaced by a maximum over $x \in \mathcal{X}$. Thus, in either case the quantity in (14) can be efficiently computed for finite alphabets.

Remark 1: To achieve a finite value for MαbeL, it is necessary that $P_Y \ll P_{Y|X=x'}$ for each $x' \in \mathcal{X}$. Failure to satisfy this condition leads to infinite leakage when $\beta > 1$.

Like other leakage measures, MαbeL satisfies several basic properties such as non-negativity, data processing inequalities and additivity, as shown in the following theorem.

Theorem 2: Let X and Y take values from finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, respectively. For $\alpha \in (1,\infty)$ and $\beta \in [1,\infty)$, MαbeL

1) is monotonically non-decreasing in β for a fixed α;
2) satisfies data processing inequalities, i.e., for the Markov chain $X - Y - Z$:

$$\mathcal{L}_{\alpha,\beta}(X \to Z) \le \mathcal{L}_{\alpha,\beta}(X \to Y) \tag{16a}$$
$$\mathcal{L}_{\alpha,\beta}(X \to Z) \le \mathcal{L}_{\alpha,\beta}(Y \to Z). \tag{16b}$$

3) is non-negative, i.e.,

$$\mathcal{L}_{\alpha,\beta}(X \to Y) \ge 0 \tag{17}$$

with equality if and only if X and Y are independent.
4) satisfies additivity: i.e., if (X_i, Y_i) for $i = 1, 2, \ldots, n$ are independent, then

$$\mathcal{L}_{\alpha,\beta}(X_1,\ldots,X_n \to Y_1,\ldots,Y_n) = \sum_{i=1}^{n} \mathcal{L}_{\alpha,\beta}(X_i \to Y_i). \tag{18}$$

A detailed proof of Theorem 2 is in Appendix B.

Remark 2: MαbeL is continuous at $(\alpha,\beta) \in [1,\infty] \times [1,\infty]$, with the exception of the point $(\alpha,\beta) = (1,1)$. The proof of this property relies on a reparameterization of MαbeL and is covered in detail in Section V.

B. Conditional MαbeL

Analogously to the connection between MαbeL and maximal leakage, we define conditional MαbeL based on conditional maximal leakage as follows.

Definition 10 (Conditional MαbeL): Let Z be the knowledge of an adversary or third-party about (X,Y). Given a conditional distribution $P_{Y|X,Z}$ (or $f_{Y|X,Z}$) and a marginal distribution P_Z (or f_Z) on supports $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$, the conditional MαbeL from X to Y given Z for $(\alpha,\beta) \in (1,\infty) \times [1,\infty)$ is defined as

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) := \sup_{P_{X|Z}} \sup_{U\to X\to Y|Z} \frac{\alpha}{(\alpha-1)\beta} \log \frac{\max_{P_{\hat{U}|Z,Y}} \mathbb{E}\left(\sum_u P_{U|Z,Y}(u|Z,Y) P_{\hat{U}|Z,Y}(u|Z,Y)^{\frac{\alpha-1}{\alpha}}\right)^{\beta}}{\max_{P_{\hat{U}|Z}} \mathbb{E}\left(\sum_u P_{U|Z}(u|Z) P_{\hat{U}|Z}(u|Z)^{\frac{\alpha-1}{\alpha}}\right)^{\beta}}. \tag{19}$$

Here $\hat{U}$ represents an estimator taking values from the same arbitrary finite alphabet as U, and the expression $U - X - Y|Z$ represents the conditional Markov chain constraint where

$$P_{UXY|Z}(u,x,y|z) = P_{X|Z}(x|z)\ P_{U|XZ}(u|x,z)\ P_{Y|XZ}(y|x,z).$$

Thus, the conditional Markov chain $U - X - Y|Z$ is equivalent to the Markov chain $U - (X,Z) - Y$. The continuous extensions can be defined analogously to Definition 9.

For a similar reason to that stated below Definition 9, the definition of conditional MαbeL in (19) recovers the definition of conditional maximal α-leakage (and thus conditional maximal leakage) for $\beta = 1$. The following theorem simplifies the expression of conditional MαbeL.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

Theorem 3: Let X, Y, and Z take values from finite supports $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, respectively. For $(\alpha, \beta) \in (1, \infty) \times [1, \infty)$, conditional M$\alpha$beL defined in (19) simplifies to

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) = \max_{z\in\mathcal{Z}} \max_{x'\in\mathcal{X}} \sup_{P_{\tilde{X}|Z}} \frac{\alpha}{(\alpha-1)\beta} \log \left[\sum_{y\in\mathcal{Y}} P_{Y|X,Z}(y|x',z)^{1-\beta} \times \left(\sum_{x\in\mathcal{X}} P_{Y|X,Z}(y|x,z)^{\alpha} P_{\tilde{X}|Z}(x|z) \right)^{\frac{\beta}{\alpha}} \right] \tag{20}$$

where $P_{\tilde{X}|Z}$ is a distribution on the support of $P_{X|Z}$.

A detailed proof of Theorem 3 is in Appendix C.

Remark 3: Interestingly, despite the fact that there is an expectation over z in the definition of conditional MαbeL, the simplified form has a maximum over z. This is in contrast to some other conditional measures in [56], [57], and [58].

Under a specific Markov chain, the following theorem shows the effect of the side information Z on leakage about any function U of X through Y.

Theorem 4: Let X, Y, and Z take values from finite alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, respectively. If $Z - X - Y$ holds, for $(\alpha, \beta) \in (1, \infty) \times [1, \infty)$, we have

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) \leq \mathcal{L}_{\alpha,\beta}(X \to Y), \tag{21}$$

with equality if for some $z \in \mathit{supp}(Z)$,

$$\mathit{supp}(X) = \mathit{supp}(X|Z = z).$$

A detailed proof of Theorem 4 is in Appendix D. Therefore, minimizing $\mathcal{L}_{\alpha,\beta}(X \to Y)$ is still a reasonable objective for a situation in which an adversary has access to side information Z which is unknown to the system designer. The following theorem shows that successive releases increase the total leakage.

Theorem 5 (Sub-Additivity/Composition): Let Z represent the side information of an adversary and X, Y_1, Y_2, and Z take values from finite supports $\mathcal{X}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$, and $\mathcal{Z}$, respectively. For $(\alpha, \beta) \in (1, \infty) \times [1, \infty)$, we have

$$\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2|Z) \leq \mathcal{L}_{\alpha,\beta}(X \to Y_1|Z) + \mathcal{L}_{\alpha,\beta}(X \to Y_2|Y_1, Z). \tag{22}$$

A detailed proof of Theorem 5 is in Appendix E.

Remark 4: In the scenario where no side information is available to an adversary, applying Theorem 5, we can show that

$$\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2) \leq \mathcal{L}_{\alpha,\beta}(X \to Y_1) + \mathcal{L}_{\alpha,\beta}(X \to Y_2|Y_1). \tag{23}$$

Combining this result with Theorem 4, we can conclude that if $Y_1 - X - Y_2$ holds, then

$$\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2) \leq \mathcal{L}_{\alpha,\beta}(X \to Y_1) + \mathcal{L}_{\alpha,\beta}(X \to Y_2). \tag{24}$$

Equation (24) recovers Liao et al.'s result [17] on the sub-additivity of maximal α-leakage, and equation (23) generalizes it.

Remark 5: Repeated use of privacy mechanisms on the outcome of previous private releases requires computing the overall privacy guarantees, a problem known as composition. A related useful property of any privacy measure, namely, composability, identifies the ease of computing this overall privacy. Let X be a sensitive random variable, $\mathcal{M}_1$ and $\mathcal{M}_2$ be privacy mechanisms,[2] and $\mathcal{M}$ be their composition. $\mathcal{M}$ is called *adaptive* if $\mathcal{M}(X) = (\mathcal{M}_1(X), \mathcal{M}_2(X, \mathcal{M}_1(X)))$, that is, the output of $\mathcal{M}_2$ depends on both X and $\mathcal{M}_1(X)$. In contrast, $\mathcal{M}$ is called *non-adaptive* if $\mathcal{M}(X) = (\mathcal{M}_1(X), \mathcal{M}_2(X))$, that is, the output of $\mathcal{M}_2$ depends on $\mathcal{M}_1(X)$ only through the random variable X. In (22), let $P_{Y_1|X,Z}$, $P_{Y_2|X,Z,Y_1}$, and $P_{Y_1,Y_2|X,Z}$ be privacy mechanisms associated with privacy measures $\mathcal{L}_{\alpha,\beta}(X \to Y_1|Z)$, $\mathcal{L}_{\alpha,\beta}(X \to Y_2|Y_1, Z)$, and $\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2|Z)$, respectively. Random variables Y_1 and Y_2 can be viewed as $\mathcal{M}_1(X)$ and $\mathcal{M}_2(X, \mathcal{M}_1(X))$, respectively. Thus, this implies that MαbeL satisfies adaptive composition. In (24), random variables Y_1 and Y_2 can be viewed as $\mathcal{M}_1(X)$ and $\mathcal{M}_2(X)$, respectively, leading to a non-adaptive composition result for MαbeL. It is known that DP and Rényi DP mechanisms also satisfy composability. In Section IV, we show that DP and Rényi DP can be recovered through conditional MαbeL. Consequently, we can employ (22) to establish bounds for the adaptive composition of Rényi DP and DP mechanisms.

IV. Relationships of Other Leakage Measures With (Conditional) MαbeL

As mentioned earlier, (conditional) MαbeL recovers (conditional) maximal α-leakage for $\beta = 1$ which simplifies to (conditional) maximal leakage for $\beta = 1$ and $\alpha \to \infty$. Moreover, in this section we show that MαbeL includes various other leakage measures, particularly, different notions of DP (see Fig. 1a).

Proposition 1: MαbeL can be simplified as follows:

- If $\alpha \leq \beta$, then
$$\mathcal{L}_{\alpha,\beta}(X \to Y) = \frac{\alpha(\beta-1)}{(\alpha-1)\beta} \mathcal{L}_{\beta}^{LRDP}(X \to Y).$$
- $\mathcal{L}_{\beta,\beta}(X \to Y) = \mathcal{L}_{\beta}^{LRDP}(X \to Y)$.
- $\mathcal{L}_{\infty,\infty}(X \to Y) = \lim_{\beta\to\infty} \lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y) = \mathcal{L}^{LDP}(X \to Y)$.

A detailed proof of Proposition 1 is in Appendix F. The key result of Proposition 1 is captured in Fig. 1a which shows that LDP (top right corner point in Fig. 1a) is the limiting point of MαbeL as $(\alpha \to \infty, \beta \to \infty)$. In particular, M$\alpha$beL reduces to maximal Rényi leakage of order β (defined in (12)) for $\alpha = \infty$ (illustrated by the gold vertical line in Fig. 1a).

Proposition 2: Conditional MαbeL can be simplified as follows:

- If $\alpha \leq \beta$, then
$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) = \max_{z,x',x} \frac{\alpha}{(\alpha-1)\beta}$$

[2]As previously mentioned, we employ the terms *privacy mechanisms* and *conditional distributions* interchangeably.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

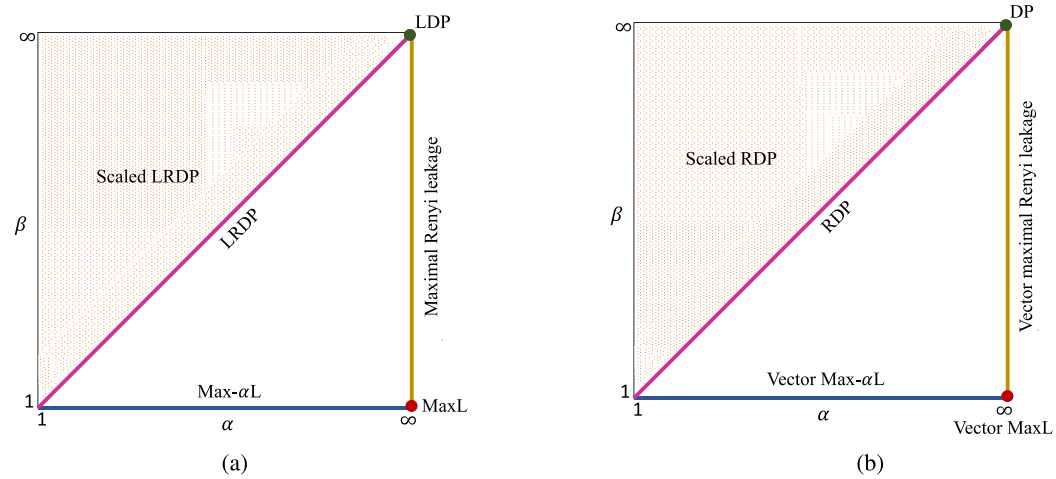


Fig. 1. Subplots 1a and 1b show the relationships between existing leakage measures with MαbeL and vector MαbeL, respectively.

$$\log \sum_y P_{Y|X,Z}(y|x',z)^{1-\beta} P_{Y|X,Z}(y|x,z)^{\beta}.$$

- If $\alpha = \beta$, then

$$\mathcal{L}_{\beta,\beta}(X \to Y|Z) = \max_{z,x',x} \frac{1}{\beta - 1} \log \sum_y P_{Y|X,Z}(y|x',z)^{1-\beta} P_{Y|X,Z}(y|x,z)^{\beta}.$$

- $\mathcal{L}_{\infty,\infty}(X \to Y|Z) = \lim_{\beta\to\infty} \lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y|Z) = \max_{z,x',y,x} \log \frac{P_{Y|X,Z}(y|x,z)}{P_{Y|X,Z}(y|x',z)}.$
- $\mathcal{L}_{\infty,\beta}(X \to Y|Z) = \max_{z,x'} \frac{1}{\beta} \log \sum_y P_{Y|X,Z}(y|x',z)^{1-\beta} \max_x P_{Y|X,Z}(y|x,z)^{\beta}.$

The proof of Proposition 2 follows from Theorem 3 and similar steps as those in the proofs of Proposition 1 and equation (15).

A. Vector MαbeL

In this section, we show that conditional MαbeL can be used to derive a general version of DP and RDP rather than their local versions (see Fig. 1b). Specifically, given a dataset with n entries, we define a vector form of MαbeL as when the adversary has access to all but one of the entries.

Definition 11 (Vector MαbeL): Let $X^n = (X_1, X_2, \ldots, X_n)$ and X_{-i} represent a dataset with n entries and all entries except the ith, respectively. Vector MαbeL is defined as

$$\mathcal{L}^{\text{vec}}_{\alpha,\beta}(X^n \to Y) := \max_i \ \mathcal{L}_{\alpha,\beta}(X_i \to Y|X_{-i}). \tag{25}$$

Proposition 3: For finite alphabets, vector MαbeL defined in (25) simplifies to

$$\mathcal{L}^{\text{vec}}_{\alpha,\beta}(X^n \to Y) = \max_{i,x_{-i},x'_i} \sup_{P_{\tilde{X}_i|X_{-i}}} \frac{\alpha}{(\alpha-1)\beta} \log \left[\sum_y P_{Y|X_i,X_{-i}}(y|x'_i,x_{-i})^{1-\beta} \left(\sum_{x_i} P_{Y|X_i,X_{-i}}(y|x_i,x_{-i})^{\alpha} P_{\tilde{X}_i|X_{-i}}(x_i|x_{-i}) \right)^{\frac{\beta}{\alpha}} \right], \tag{26}$$

where $P_{\tilde{X}_i|X_{-i}}$ is a distribution on the support of $P_{X_i|X_{-i}}$. Moreover, it recovers

- vector maximal α-leakage (and thus vector maximal leakage) when $\beta = 1$, that is,

$$\mathcal{L}^{\text{vec}}_{\alpha,1}(X^n \to Y) = \max_{i,x_{-i}} \sup_{P_{\tilde{X}_i|X_{-i}}} \frac{\alpha}{\alpha - 1} \log \sum_y \left[\sum_{x_i} P_{Y|X_i,X_{-i}}(y|x_i,x_{-i})^{\alpha} P_{\tilde{X}_i|X_{-i}}(x_i|x_{-i}) \right]^{\frac{1}{\alpha}} \tag{27}$$

- a scaled RDP of order β when $\alpha \le \beta$, that is,

$$\mathcal{L}^{\text{vec}}_{\alpha,\beta}(X^n \to Y) = \max_{x^n \sim x'^n} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X^n}(y|x'^n)^{1-\beta} P_{Y|X^n}(y|x^n)^{\beta}; \tag{28}$$

- RDP of order $\alpha = \beta$ when $\alpha = \beta$, that is,

$$\mathcal{L}^{\text{vec}}_{\alpha=\beta}(X^n \to Y) = \max_{x^n \sim x'^n} \frac{1}{\beta - 1} \log \sum_y P_{Y|X^n}(y|x'^n)^{1-\beta} P_{Y|X^n}(y|x^n)^{\beta}; \tag{29}$$

- DP when $\alpha, \beta \to \infty$;
- a variant of RDP of order β for $\alpha \to \infty$ and an arbitrary β, which we call *vector maximal Rényi leakage*. That is,

$$\mathcal{L}^{\text{vec}}_{\infty,\beta}(X^n \to Y) = \max_{i,x'_i,x_{-i}} \frac{1}{\beta} \log \left[\sum_y P_{Y|X_i,X_{-i}}(y|x'_i,x_{-i})^{1-\beta} \times \max_{x_i} P_{Y|X_i,X_{-i}}(y|x_i,x_{-i})^{\beta} \right]. \tag{30}$$

We remark that vector maximal Rényi leakage defined in (30) differs from RDP of order β mainly in that the max over x_i is inside the summation over y rather than outside. A detailed proof of Proposition 3 can be found in Appendix G.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

V. Maximal (α, τ)-Leakage: A Reparameterization of MαbeL

Maximal (α, β)-leakage is not uniquely defined at $\alpha = \beta = 1$. As $\alpha = \beta \to 1$, it can be verified using L'Hôpital's rule that maximal $(\alpha = \beta)$-leakage, i.e., local Rényi DP, simplifies to

$$\max_{x,x'} D_{KL}\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x')\right)$$

whereas the limit of maximal $(\alpha, \beta = 1)$-leakage, i.e., maximal α-leakage, gives Shannon channel capacity as $\alpha \to 1$ [17]. In this section, we consider a reparameterization which leads to a new measure. The new measure is uniquely defined in all its endpoints and it is monotonic in both orders (unlike maximal (α, β)-leakage which is monotonic in only one of its orders). Let $\tau \in [1, \infty)$ and $\beta = \frac{\alpha\tau}{\tau+\alpha-1}$, where $\alpha \in (1, \infty)$. We may re-write the expression of maximal (α, β)-leakage in (14) in terms of α and τ, as follows.

$$\begin{aligned}&\mathcal{L}_{\alpha,\tau}(X \to Y)\\ &= \max_{x'} \sup_{P_{\tilde{X}}} \left(\frac{1}{\alpha-1} + \frac{1}{\tau}\right) \log \left[\sum_y P_{Y|X}(y|x')^{\frac{(\tau-1)(1-\alpha)}{\tau+\alpha-1}}\right.\\ &\left.\times \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha}\right)^{\frac{\tau}{\tau+\alpha-1}}\right]. \end{aligned} \tag{31}$$

This measure is defined by its continuous extension for $(\alpha, \tau) \in \{1, \infty\} \times [1, \infty)$ and $(\alpha, \tau) \in (1, \infty) \times \{\infty\}$. It is also defined by $\lim_{\tau\to\infty} \lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\tau}(X \to Y)$ and $\lim_{\tau\to\infty} \lim_{\alpha\to 1} \mathcal{L}_{\alpha,\tau}(X \to Y)$ for $(\alpha = \infty, \tau = \infty)$ and $(\alpha = 1, \tau = \infty)$, respectively. We call the quantity in (31) *maximal (α, τ)-leakage*. It is important to note that β is non-decreasing in τ for a fixed α and so $\alpha > \beta$ (if $\tau \to \infty$, then $\beta \to \alpha$, see Fig. 2a).

Lemma 1: For $(\alpha, \tau) \in (1, \infty) \times [1, \infty)$, maximal (α, τ)-leakage can be represented by

$$\begin{aligned}&\mathcal{L}_{\alpha,\tau}(X \to Y)\\ &= \max_{x'} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \frac{1}{\alpha-1} \log \left[\sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha}\right.\\ &\left.\times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}\right)^{1-\alpha}\right], \end{aligned} \tag{32}$$

and it is non-decreasing in τ and α for a fixed α and τ, respectively.

A detailed proof is in Appendix H.

Remark 6: Some of the relationships to other measures become clear from this lemma. Namely, if $\tau = 1$, then we see the expression of maximal α-leakage in terms of Sibson mutual information, that is,

$$\sup_{P_{\tilde{X}}} \inf_{Q_Y} D_\alpha(P_{\tilde{X}} \times P_{Y|X} \| P_{\tilde{X}} \times Q_Y) = \sup_{P_{\tilde{X}}} I_\alpha^S(\tilde{X}; Y). \tag{33}$$

If $\tau \to \infty$, then we see the definition of LRDP as

$$\max_{x,x'} D_\alpha(P_{Y|X=x} \| P_{Y|X=x'}). \tag{34}$$

Note that $\frac{\tau}{\tau+\alpha-1} < 1$ for $\tau \in [1, \infty)$ and $\alpha \in (1, \infty)$, and so the quantity inside the logarithm in (31) is concave in $P_{\tilde{X}}$. Now we consider some endpoints of α and τ values (see Fig. 2b). If $\tau = 1$, then we recover maximal α-leakage which reduces to maximal leakage when $\alpha = \infty$.

If $\tau = \infty$, then we recover local Rényi differential privacy of order α which simplifies to local differential privacy for $\alpha = \infty$. If $\alpha = \infty$, then we recover maximal Rényi leakage of order τ, that is,

$$\begin{aligned}&\mathcal{L}_{\alpha=\infty,\tau}(X \to Y)\\ &= \max_{x'} \frac{1}{\tau} \log \sum_y P_{Y|X}(y|x')^{1-\tau} \max_x P_{Y|X}(y|x)^{\tau}. \end{aligned} \tag{35}$$

Following similar steps as those in the proof of Proposition 1, we can also show that

$$\begin{aligned}\mathcal{L}_{\alpha=\infty,\tau=\infty}(X \to Y) &= \lim_{\tau\to\infty} \lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\tau}(X \to Y)\\ &= \mathcal{L}^{\text{LDP}}(X \to Y). \end{aligned} \tag{36}$$

Proposition 4: For $\alpha \to 1$, maximal (α, τ)-leakage simplifies to

$$\begin{aligned}\mathcal{L}_{\alpha=1,\tau}(X \to Y) = \max_{x'} \sup_{P_{\tilde{X}}} &\left[\frac{1}{\tau} I(\tilde{X}; Y)\right.\\ &\left.+ \left(1 - \frac{1}{\tau}\right) D_{KL}\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x') | P_{\tilde{X}}(x)\right)\right]. \end{aligned} \tag{37}$$

We call the quantity in (37) the *τ-Shannon leakage*. A detailed proof of Proposition 4 is in Appendix I.

Remark 7: For $\tau \to \infty$, τ-Shannon leakage simplifies to

$$\begin{aligned}&\mathcal{L}_{\alpha=1,\tau=\infty}(X \to Y)\\ &= \lim_{\tau\to\infty} \lim_{\alpha\to 1} \mathcal{L}_{\alpha,\tau}(X \to Y) && (38)\\ &= \max_{x'} \sup_{P_{\tilde{X}}} D_{KL}\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x') | P_{\tilde{X}}(x)\right) && (39)\\ &= \max_{x,x'} D_{KL}\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x')\right). && (40) \end{aligned}$$

(40) follows because $D_{KL}\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x') | P_{\tilde{X}}(x)\right)$ is linear in $P_{\tilde{X}}$ and so the supremum is attained at an extreme point. This quantity is KL divergence. Also, for $\tau = 1$, τ-Shannon leakage is given by

$$\mathcal{L}_{\alpha=1,\tau=1}(X \to Y) = \sup_{P_{\tilde{X}}} I(\tilde{X}; Y) \tag{41}$$

which is Shannon channel capacity. So τ-Shannon leakage smoothly tunes between KL divergence ($\tau = \infty$) and Shannon channel capacity ($\tau = 1$).

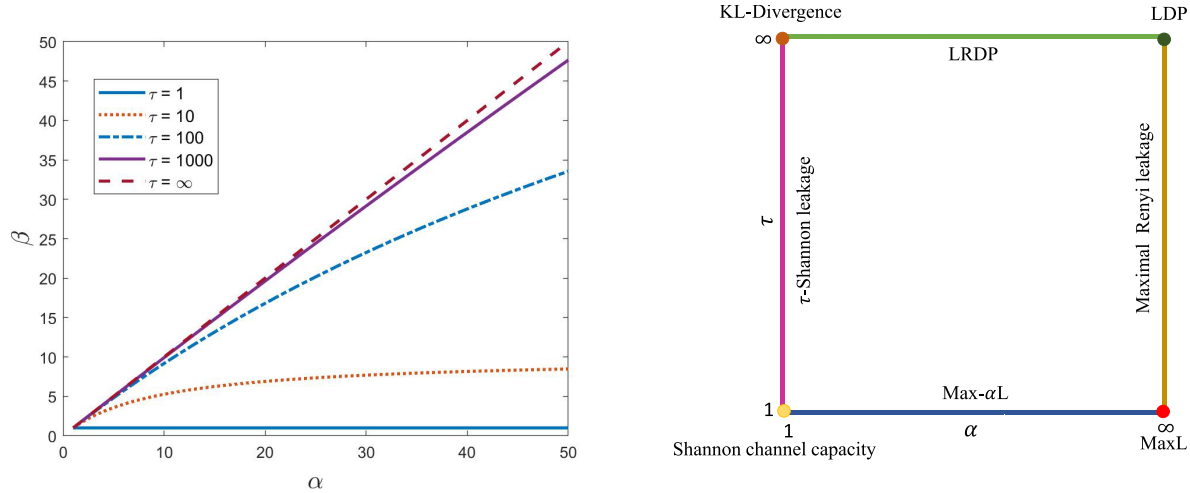
Theorem 6: Let $P_Y \ll P_{Y|X=x'}$ for each $x' \in \mathcal{X}$. Maximal (α, τ)-leakage is continuous in (α, τ) for all $(\alpha, \tau) \in [1, \infty] \times [1, \infty]$, and M$\alpha$beL is continuous in (α, β) for all $(\alpha, \beta) \in [1, \infty] \times [1, \infty] \setminus \{(1, 1)\}$.

The proof of Theorem 6 can be found in Appendix J. Similar to the definition of vector MαbeL, maximal (α, τ)-leakage can be generalized to a vector form.

VI. Continuous Alphabets

In this section, we generalize Theorem 1 and Theorem 3 to continuous alphabets.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.



(a) (b)

Fig. 2. Subplot 2a shows β vs α curves across different τ values. Subplot 2b shows relationship between maximal (α, τ)-leakage and other leakage measures as a function of α and τ.

Theorem 7: Let X and Y be continuous random variables having a continuous joint pdf f_{XY}. MαbeL defined in (13) simplifies to

$$\mathcal{L}_{\alpha,\beta}(X \to Y) = \max_{x':f_X(x')>0} \sup_{f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_{Y|X}(y|x')^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} dx \right)^{\beta/\alpha} dy, \tag{42}$$

where $f_{\tilde{X}}$ is a pdf on $\mathcal{X}$.

The proof of Theorem 7 and expressions similar to (42) for the other cases, i.e., for discrete X and continuous Y, and continuous X and discrete Y can be found in Appendix K.

Theorem 8: Let X, Y, and Z be continuous random variables having a continuous joint pdf f_{XYZ}. The conditional MαbeL defined in (19) simplifies to

$$\begin{aligned}&\mathcal{L}_{\alpha,\beta}(X \to Y|Z)\\ &= \max_{z} \max_{x'} \sup_{f_{\tilde{X}|Z=z}} \frac{\alpha}{(\alpha-1)\beta} \log \left[\int_{\mathcal{Y}} f_{Y|X,Z}(y|x',z)^{1-\beta} \right.\\ &\left. \times \left(\int_{\mathcal{X}} f_{Y|X,Z}(y|x,z)^{\alpha} f_{\tilde{X}|Z=z}(x)\, dx \right)^{\frac{\beta}{\alpha}} dy \right]\end{aligned} \tag{43}$$

where $f_{\tilde{X}|Z=z}$ is a pdf on the support of $f_{X|Z=z}$ for any z that $f_Z(z) > 0$.

The proof of Theorem 8 follows a similar approach to the proof of Theorem 7, and expressions similar to (43) for the other cases, i.e., for discrete X and continuous Y, and continuous X and discrete Y, can be derived similarly. Moreover, by applying similar steps to the proof of Proposition 1, we can recover RDP, DP, and vector maximal Rényi leakage as special cases of vector MαbeL for continuous alphabets.

A. Results for Known Mechanisms

In this section, we show how vector MαbeL relaxes differential privacy through vector maximal Rényi leakage under Gaussian and Laplacian mechanisms (see Fig. 3). The proofs for this section can be found in Appendix L.

Proposition 5: Let $h : \mathcal{X}^n \to \mathbb{R}$ be a real-valued function such that for all $i, x_{-i}, x_i, \tilde{x}_i$ we have $|h(x_{-i}, x_i) - h(x_{-i}, \tilde{x}_i)| \leq \delta$, where $x^n = \{x_{-i}, x_i\}$ and $\tilde{x}^n = \{x_{-i}, \tilde{x}_i\}$ are neighboring datasets, and δ is a sensitivity parameter. For $\beta \in (1, \infty)$,

- if $\mathcal{M}(x^n) = h(x^n) + N$ where $N \sim Lap\,(0, b)$, then

$$\mathcal{L}^{\text{vec}}_{\infty,\beta}(X^n \to M(X^n)) \leq \frac{1}{\beta} \log \left[\frac{1}{2} - \frac{1}{2(\beta-1)} + \left(\frac{1}{2} + \frac{1}{2(\beta-1)} \right) \exp\left(\frac{(\beta-1)\delta}{b} \right) \right]; \tag{44}$$

- if $\mathcal{M}(x^n) = h(x^n) + N$ where $N \sim \mathcal{N}(0, \sigma^2)$, then

$$\begin{aligned}&\mathcal{L}^{\text{vec}}_{\infty,\beta}(X^n \to M(X^n))\\ &\leq \frac{1}{\beta} \log \left[\frac{1}{2} + \frac{1}{2\sqrt{\beta-1}} \operatorname{erfi}\left(\sqrt{\frac{\beta-1}{2\sigma^2}}\, \delta \right) \right.\\ &\left. + \frac{1}{2} \exp\left(\frac{\beta(\beta-1)\delta^2}{2\sigma^2} \right) \left(1 + \operatorname{erf}\left(\frac{(\beta-1)\delta}{\sqrt{2}\sigma} \right) \right) \right],\end{aligned} \tag{45}$$

where erf indicates the error function, that is, $\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2}\, dt$, and erfi indicates the imaginary error function, that is, $\operatorname{erfi}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{t^2}\, dt$.

Both upper bounds are achieved with equality if there exist i and x_{-i} such that the function $h(x_{-i}, x_i)$ is surjective in x_i and $\max_{x_i, \tilde{x}_i} |h(x_{-i}, x_i) - h(x_{-i}, \tilde{x}_i)| = \delta$.

For $n = 1$, the upper bounds on vector maximal Rényi leakage in (44) and (45) collapse to upper bounds on maximal Rényi leakage under Laplacian and Gaussian mechanisms, respectively.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

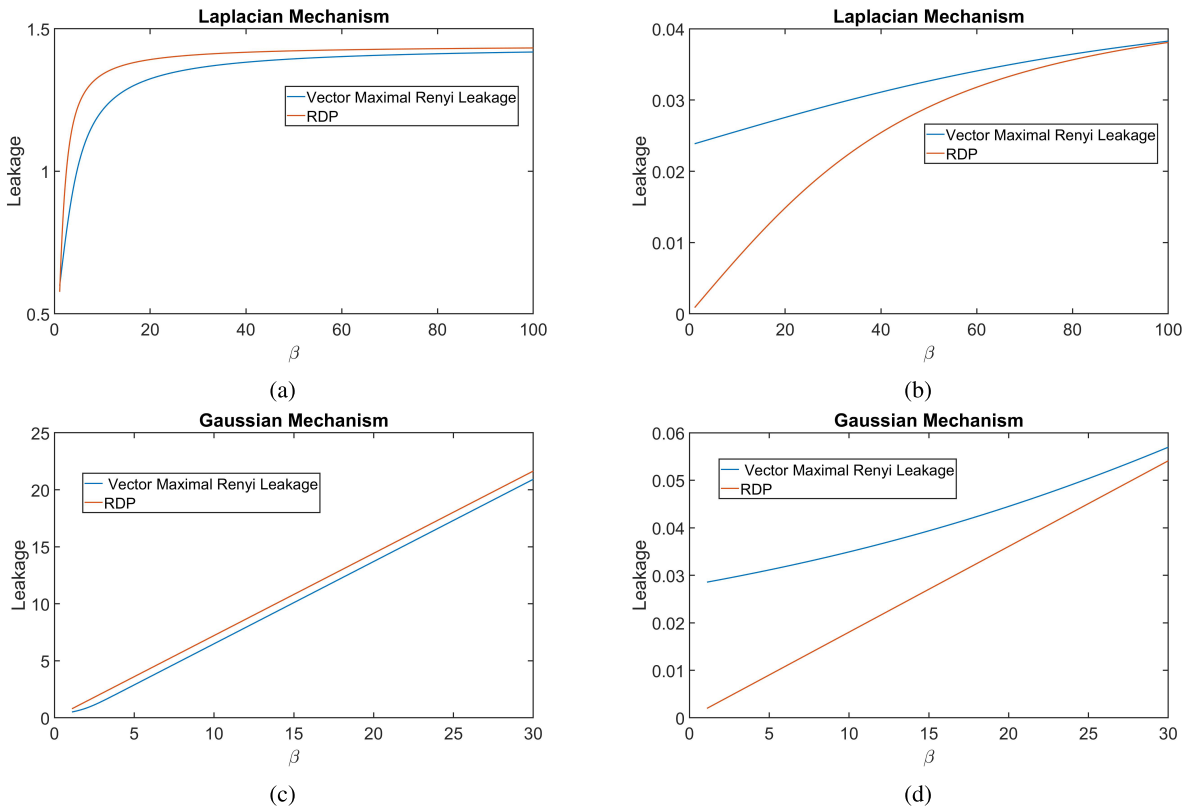


Fig. 3. Subplots 3a and 3b compare vector maximal Renyi leakage and Renyi differential privacy under Laplacian mechanisms with $b = 1$ and $b = 30$, respectively. Subplots 3c and 3d compare vector maximal Renyi leakage and Renyi differential privacy under Gaussian mechanisms with $\sigma = 1$ and $\sigma = 20$, respectively. In all subplots, we consider a situation in which the upper bounds (44) and (45) are achieved with equality, and the sensitivity parameter is 1.

VII. Conclusion

In this paper, we have introduced a new measure of information leakage called maximal (α, β)-leakage that bridges several existing leakage measures, including maximal α-leakage ($\beta = 1$), maximal leakage ($\alpha = \infty, \beta = 1$), (local) differential privacy ($\alpha = \infty, \beta = \infty$), (local) Rényi differential privacy ($\alpha = \beta$), and a variant of RDP, which we call vector maximal Rényi leakage ($\alpha = \infty$). This provides a much-needed operational interpretation to (local) RDP. We believe that our work has taken a step towards identifying the common characteristics of various information leakage measures despite their diversity. For example, our formulation allows us to smoothly transition from average-case leakage measures to worst-case leakage measures by exploiting the interplay between the parameters α and β. Finally, we posit that the unification provided by our guessing framework allows us to tailor the proposed leakage measure to study privacy-utility tradeoffs under different settings depending on the context.

Appendix A
Proof of Theorem 1

For $\alpha \in (1, \infty)$ and $\beta \in [1, \infty)$, we first bound $\mathcal{L}_{\alpha,\beta}(X \to Y)$ from above and then, give an achievable scheme.

Upper Bound: Consider the optimization in the denominator of (13):

$$\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)^{\frac{\alpha-1}{\alpha}}. \tag{46}$$

This is solved by

$$P_U(u) P_{\hat{U}}(u)^{-1/\alpha} = \nu \tag{47}$$

for some constant ν. So we have

$$P_{\hat{U}}(u) = \frac{P_U(u)^\alpha}{\sum_{u'} P_U(u')^\alpha}. \tag{48}$$

Thus the denominator becomes

$$\sum_u P_U(u) \left(\frac{P_U(u)^\alpha}{\sum_{u'} P_U(u')^\alpha} \right)^{\frac{\alpha-1}{\alpha}} = \left(\sum_u P_U(u)^\alpha \right)^{\frac{1}{\alpha}}. \tag{49}$$

Similarly, the numerator becomes

$$\left[\sum_y P_Y(y) \left(\sum_u P_{U|Y}(u|y)^\alpha \right)^{\beta/\alpha} \right]^{1/\beta}. \tag{50}$$

Thus, the logarithmic term in (13) reduces to

$$\log \frac{\left[\sum_y P_Y(y) \left(\sum_u P_{U|Y}(u|y)^\alpha \right)^{\beta/\alpha} \right]^{1/\beta}}{\left(\sum_u P_U(u)^\alpha \right)^{1/\alpha}} \tag{51}$$

$$= \log \frac{\left[\sum_y P_Y(y)^{1-\beta} \left(\sum_u P_{U,Y}(u,y)^\alpha \right)^{\beta/\alpha} \right]^{1/\beta}}{\left(\sum_u P_U(u)^\alpha \right)^{1/\alpha}} \tag{52}$$

$$= \frac{1}{\beta} \log \sum_y P_Y(y)^{1-\beta} \left(\frac{\sum_u P_U(u)^\alpha P_{Y|U}(y|u)^\alpha}{\sum_u P_U(u)^\alpha} \right)^{\frac{\beta}{\alpha}}. \tag{53}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

Using Jensen's inequality and the Markov chain $U - X - Y$, we have

$$P_{Y|U}(y|u)^\alpha = \left(\sum_x P_{X|U}(x|u)P_{Y|X}(y|x)\right)^\alpha \tag{54}$$

$$\leq \sum_x P_{X|U}(x|u)P_{Y|X}(y|x)^\alpha. \tag{55}$$

So MαbeL may be bounded from above by

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) \\
&\leq \sup_{P_X} \sup_{U \to X \to Y} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_Y(y)^{1-\beta} \\
&\quad \times \left(\frac{\sum_{u,x} P_U(u)^\alpha P_{X|U}(x|u)P_{Y|X}(y|x)^\alpha}{\sum_u P_U(u)^\alpha}\right)^{\frac{\beta}{\alpha}} \qquad (56)\\
&\leq \sup_{P_X} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_Y(y)^{1-\beta} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x)P_{Y|X}(y|x)^\alpha\right)^{\frac{\beta}{\alpha}} \qquad (57)
\end{aligned}$$

where

$$P_{\tilde{X}}(x) = \frac{\sum_u P_U(u)^\alpha P_{X|U}(x|u)}{\sum_u P_U(u)^\alpha}. \tag{58}$$

Lower Bound: The proof is based on the expression in (53) as well as "shattering" method. Consider a random variable U such that $U \to X \to Y$ form a Markov chain and $H(X|U) = 0$. For each x, let $\mathcal{U}_x$ be a finite set such that $U = u \in \mathcal{U}_x$ if and only if $X = x$ and $\mathcal{U} = \bigcup_{x\in\mathcal{X}} \mathcal{U}_x$. Moreover, given $X = x$ let U be uniformly distributed on $\mathcal{U}_x$. That is,

$$P_{U|X}(u|x) = \begin{cases} \frac{1}{|\mathcal{U}_x|} & \text{for all } u \in \mathcal{U}_x \\ 0 & \text{otherwise,} \end{cases} \tag{59}$$

and so

$$P_{Y|U}(y|u) = \begin{cases} P_{Y|X}(y|x) & \text{for all } u \in \mathcal{U}_x \\ 0 & \text{otherwise.} \end{cases} \tag{60}$$

Therefore, we have

$$\frac{\sum_u P_U(u)^\alpha P_{Y|U}(y|u)^\alpha}{\sum_u P_U(u)^\alpha} \tag{61}$$

$$= \frac{\sum_{x\in\mathcal{X}} \sum_{u\in\mathcal{U}_x} \left(\frac{P_X(x)P_{U|X}(u|x)}{P_{X|U}(x|u)}\right)^\alpha P_{Y|U}(y|u)^\alpha}{\sum_{x\in\mathcal{X}} \sum_{u\in\mathcal{U}_x} \left(\frac{P_X(x)P_{U|X}(u|x)}{P_{X|U}(x|u)}\right)^\alpha} \tag{62}$$

$$= \frac{\sum_x |\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha P_{Y|X}(y|x)^\alpha}{\sum_x |\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha}. \tag{63}$$

So we may bound MαbeL from below by

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) \\
&\geq \sup_{P_X} \sup_{\mathcal{U}_x} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_Y(y)^{1-\beta} \\
&\quad \times \left(\frac{\sum_x |\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha P_{Y|X}(y|x)^\alpha}{\sum_x |\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha}\right)^{\frac{\beta}{\alpha}} \qquad (64)\\
&= \sup_{P_X} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_Y(y)^{1-\beta} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x)P_{Y|X}(y|x)^\alpha\right)^{\frac{\beta}{\alpha}} \qquad (65)
\end{aligned}$$

where

$$P_{\tilde{X}}(x) = \frac{|\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha}{\sum_x |\mathcal{U}_x|^{1-\alpha} P_X(x)^\alpha}, \tag{66}$$

and we have used the fact that any distribution $P_{\tilde{X}}(x)$ can be reached with appropriate choice of $|\mathcal{U}_x|$, assuming $P_X(x) > 0$ for all x; this condition can be assumed because any P_X is arbitrarily close to a distribution with full support. Thus, combining (57) and (65), we have

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) = \sup_{P_X} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \\
&\log \sum_y P_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x)P_{Y|X}(y|x)^\alpha\right)^{\frac{\beta}{\alpha}}. \qquad (67)
\end{aligned}$$

Note that the choice of P_X only impacts P_Y, and the quantity inside the log is convex in P_Y. Since the supremum of a convex function is attained at an extreme point, we may simplify (67) as follows.

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) = \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \\
&\log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{\tilde{X}}(x)P_{Y|X}(y|x)^\alpha\right)^{\beta/\alpha}. \qquad (68)
\end{aligned}$$

We now obtain the expression of maximal Rényi leakage. We first bound maximal Rényi leakage from above as follows.

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) \\
&= \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x)\ P_{Y|X}(y|x)^\alpha\right)^{\beta/\alpha} \qquad (69)\\
&\leq \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x)\ \max_x P_{Y|X}(y|x)^\alpha\right)^{\beta/\alpha} \qquad (70)\\
&= \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \left(\max_x P_{Y|X}(y|x)^\alpha \sum_x P_{\tilde{X}}(x)\right)^{\beta/\alpha} \qquad (71)\\
&= \frac{\alpha}{(\alpha-1)\beta} \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \max_x P_{Y|X}(y|x)^\beta. \qquad (72)
\end{aligned}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

So

$$\lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y) \leq \frac{1}{\beta} \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^{\beta}. \quad (73)$$

We now provide an achievable scheme. We have

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) \\
&= \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x)\ P_{Y|X}(y|x)^{\alpha} \right)^{\beta/\alpha} && (74)\\
&\geq \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times \left(P_{\tilde{X}}(x_y^*)\ P_{Y|X}(y|x_y^*)^{\alpha}\right)^{\beta/\alpha} && (75)\\
&\geq \frac{\alpha}{(\alpha-1)\beta} \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \\
&\quad \times\ |\mathcal{X}|^{-\frac{\beta}{\alpha}}\ P_{Y|X}(y|x_y^*)^{\beta} && (76)\\
&= \frac{\alpha}{(\alpha-1)\beta} \max_{x'} \Bigg[\log |\mathcal{X}|^{-\frac{\beta}{\alpha}} \\
&\quad + \log \sum_y P_{Y|X}(y|x')^{1-\beta}\ P_{Y|X}(y|x_y^*)^{\beta} \Bigg] && (77)\\
&= -\frac{1}{\alpha-1} \log |\mathcal{X}| + \frac{\alpha}{(\alpha-1)\beta} \\
&\quad \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta}\ P_{Y|X}(y|x_y^*)^{\beta} && (78)\\
&= -\frac{1}{\alpha-1} \log |\mathcal{X}| + \frac{\alpha}{(\alpha-1)\beta} \\
&\quad \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^{\beta} && (79)
\end{aligned}$$

where $x_y^* = \arg\max_x P_{Y|X}(y|x)$ for $y \in \mathcal{Y}$. So

$$\lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y) \geq \frac{1}{\beta} \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^{\beta}. \quad (80)$$

Combining (73) and (80), we get

$$\lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y) = \frac{1}{\beta} \max_{x'} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^{\beta}. \quad (81)$$

Appendix B
Proof of Theorem 2

Monotonicity in β: For $\alpha \in (1,\infty)$, $\beta_1, \beta_2 \in [1,\infty)$ and $\beta_2 > \beta_1$, consider the argument of the logarithm in (14):

$$\begin{aligned}
&\sum_y P_{Y|X}(y|x')^{1-\beta_1} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{\beta_1}{\alpha}} && (82)\\
&= \sum_y P_{Y|X}(y|x') \Bigg(P_{Y|X}(y|x')^{-\alpha} \\
&\quad \times \sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \Bigg)^{\frac{\beta_2\beta_1}{\alpha\beta_2}} && (83)\\
&\leq \Bigg(\sum_y P_{Y|X}(y|x') \Bigg(P_{Y|X}(y|x')^{-\alpha} \\
&\quad \times \sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \Bigg)^{\frac{\beta_2}{\alpha}} \Bigg)^{\frac{\beta_1}{\beta_2}} && (84)\\
&= \Bigg(\sum_y P_{Y|X}(y|x')^{1-\beta_2} \Bigg(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \Bigg)^{\frac{\beta_2}{\alpha}} \Bigg)^{\frac{\beta_1}{\beta_2}} && (85)
\end{aligned}$$

where the inequality results from applying Jensen's inequality to the concave function $f:\ x \to x^p\ (x \geq 0,\ p < 1)$. For $\alpha \in (1,\infty)$ and $\beta \in [1,\infty)$, the function $f: t \to \frac{\alpha}{(\alpha-1)\beta} \log t$ is increasing in $t > 0$. Therefore, we have

$$\begin{aligned}
&\frac{\alpha}{(\alpha-1)\beta_1} \log \sum_y P_{Y|X}(y|x')^{1-\beta_1} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{\beta_1}{\alpha}} && (86)\\
&\leq \frac{\alpha}{(\alpha-1)\beta_2} \log \sum_y P_{Y|X}(y|x')^{1-\beta_2} \\
&\quad \times \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{\beta_2}{\alpha}}. && (87)
\end{aligned}$$

Taking the maximum over x' and supremum over $P_{\tilde{X}}$ completes the proof. Another way to prove this property is to consider the numerator in (13) as the β-norm of a random variable. Since the β-norm of a random variable is non-decreasing in β, maximal (α,β)-leakage is non-decreasing in β.

Data processing inequalities: Let random variables X, Y, Z form a Markov chain, i.e., $X - Y - Z$. Based on the expression of maximal (α,β)-leakage in (67) we first prove the post-processing inequality, that is

$$\mathcal{L}_{\alpha,\beta}(X \to Z) \leq \mathcal{L}_{\alpha,\beta}(X \to Y). \quad (88)$$

For any $y \in \mathcal{Y}$, let

$$g(y) = \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{1}{\alpha}} \quad (89)$$

and

$$c_z(y) = \frac{P_Y(y)\ P_{Z|Y}(z|y)}{P_Z(z)} \quad (90)$$

such that $\sum_y c_z(y) = 1$. We have

$$\begin{aligned}
&\sum_y P_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{\beta}{\alpha}} && (91)\\
&= \sum_y P_Y(y)^{1-\beta} g(y)^{\beta} && (92)\\
&= \sum_{y,z} P_Y(y) P_{Z|Y}(z|y) \left(\frac{g(y)}{P_Y(y)} \right)^{\beta} && (93)
\end{aligned}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \sum_z P_Z(z) \sum_y c_z(y) \left(\frac{g(y)}{P_Y(y)}\right)^\beta \tag{94}$$

$$\geq \sum_z P_Z(z) \left(\sum_y c_z(y) \frac{g(y)}{P_Y(y)}\right)^\beta \tag{95}$$

$$= \sum_z P_Z(z)^{1-\beta} \left(\sum_y P_{Z|Y}(z|y) g(y)\right)^\beta \tag{96}$$

where (95) follows from applying Jensen's inequality to the convex function $f:\ x \to x^p$ $(x \geq 0,\ p \geq 1)$. Recalling the definition of $g(y)$ from (89), we have

$$\sum_y P_{Z|Y}(z|y) g(y) \tag{97}$$

$$= \sum_y P_{Z|Y}(z|y) \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^\alpha\right)^{\frac{1}{\alpha}} \tag{98}$$

$$= \sum_y \left(\sum_x \left(P_{\tilde{X}}(x)^{\frac{1}{\alpha}} P_{Z|Y}(z|y) P_{Y|X}(y|x)\right)^\alpha\right)^{\frac{1}{\alpha}} \tag{99}$$

$$\geq \left(\sum_x \left(\sum_y P_{\tilde{X}}(x)^{\frac{1}{\alpha}} P_{Z|Y}(z|y) P_{Y|X}(y|x)\right)^\alpha\right)^{\frac{1}{\alpha}} \tag{100}$$

$$= \left(\sum_x P_{\tilde{X}}(x) P_{Z|X}(z|x)^\alpha\right)^{\frac{1}{\alpha}} \tag{101}$$

where

- (100) follows because p-norm satisfies the triangle inequality for $p \in (1, \infty)$,
- (101) follows because the Markov chain $X - Y - Z$ holds.

Applying (101) to (96), and using the fact that for $\alpha \in (1, \infty)$ and $\beta \in [1, \infty)$, the function $f: t \to \frac{\alpha}{(\alpha-1)\beta} \log t$ is increasing in $t > 0$, gives

$$\frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^\alpha\right)^{\frac{\beta}{\alpha}}$$
$$\geq \frac{\alpha}{(\alpha-1)\beta} \log \sum_z P_Z(z)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Z|X}(z|x)^\alpha\right)^{\frac{\beta}{\alpha}}. \tag{102}$$

Taking suprema over P_X and $P_{\tilde{X}}$ completes the proof.

We now prove the linkage inequality, that is

$$\mathcal{L}_{\alpha,\beta}(X \to Z) \leq \mathcal{L}_{\alpha,\beta}(Y \to Z), \tag{103}$$

using the definition of maximal (α, β)-leakage in (13). Let

$$f(P_{UZ}) = \frac{\alpha}{\alpha - 1} \log \frac{\max_{P_{\hat{U}|Z}} \left[\sum_z P_Z(z) \left(\sum_u P_{U|Z}(u|z) P_{\hat{U}|Z}(u|z)^{\frac{\alpha-1}{\alpha}}\right)^\beta\right]^{1/\beta}}{\max_{P_{\hat{U}}} \sum_u P_U(u) P_{\hat{U}}(u)^{\frac{\alpha-1}{\alpha}}}. \tag{104}$$

For the Markov chain $X - Y - Z$, we have

$$\mathcal{L}_{\alpha,\beta}(X \to Z) = \sup_{P_X} \sup_{U \to X \to Z} f(P_{UZ}) \tag{105}$$
$$= \sup_{P_X} \sup_{U \to X \to Y \to Z} f(P_{UZ}) \tag{106}$$
$$\leq \sup_{P_X} \sup_{U \to Y \to Z} f(P_{UZ}) \tag{107}$$
$$\leq \sup_{P_Y} \sup_{U \to Y \to Z} f(P_{UZ}) \tag{108}$$
$$= \mathcal{L}_{\alpha,\beta}(Y \to Z)$$

where (106) follows because P_{UZ} are the same under the Markov chains $U - X - Z$ and $U - X - Y - Z$, and (108) follows from the fact that a subset of all distributions P_Y is reachable from the distribution P_X.

Non-negativity: Consider the logarithmic term in (14):

$$\log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^\alpha\right)^{\frac{\beta}{\alpha}} \tag{109}$$

$$\geq \log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)\right)^\beta \tag{110}$$

$$= \log \sum_y P_{Y|X}(y|x') \left(\frac{\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)}{P_{Y|X}(y|x')}\right)^\beta \tag{111}$$

$$\geq \log \left(\sum_y P_{Y|X}(y|x') \frac{\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)}{P_{Y|X}(y|x')}\right)^\beta \tag{112}$$

$$= \log \left(\sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)\right)^\beta = \log 1 = 0 \tag{113}$$

where both inequalities follow from applying Jensen's inequality to the convex function $f:\ x \to x^p$ $(x \geq 0,\ p \geq 1)$ and the fact that logarithmic functions are increasing. Equality holds in the first inequality if and only if for any $y \in \mathcal{Y}$, $P_{Y|X}(y|x)$ are the same for all $x \in \mathcal{X}$. Thus, we have

$$P_{Y|X}(y|x) = P_Y(y) \quad x \in \mathcal{X}, y \in \mathcal{Y} \tag{114}$$

which means X and Y are independent. This condition is also sufficient for equality in the second inequality.

Additivity: We first prove additivity for $n = 2$. We have $P_{X_1Y_1X_2Y_2} = P_{X_1Y_1} \cdot P_{X_2Y_2}$. To prove the additivity in (18), using Theorem 1 it suffices to show that

$$\sup_{P_{\tilde{X}_1,\tilde{X}_2}} \sum_{y_1,y_2} P_{Y_1Y_2|X_1X_2}(y_1,y_2|x_1',x_2')^{1-\beta} \times \left(\sum_{x_1,x_2} P_{\tilde{X}_1,\tilde{X}_2}(x_1,x_2) P_{Y_1Y_2|X_1X_2}(y_1,y_2|x_1,x_2)^\alpha\right)^{\beta/\alpha} \tag{115}$$

$$= \sup_{\substack{P_{\tilde{X}_i} \\ i \in 1,2}} \prod_{i=1}^{2} \left(\sum_{y_i} P_{Y|X}(y_i|x_i')^{1-\beta} \times \left(\sum_{x_i} P_{\tilde{X}_i}(x_i) P_{Y_i|X_i}(y_i|x_i)^\alpha\right)^{\beta/\alpha}\right), \tag{116}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

for every x_1', x_2'. We simplify LHS in (115) as

$$\sup_{P_{\tilde{X}_1,\tilde{X}_2}} \sum_{y_1,y_2} P_{Y_1Y_2|X_1X_2}(y_1,y_2|x_1',x_2')^{1-\beta} \times \Big(\sum_{x_1,x_2} P_{\tilde{X}_1,\tilde{X}_2}(x_1,x_2)P_{Y_1Y_2|X_1X_2}(y_1,y_2|x_1,x_2)^{\alpha}\Big)^{\beta/\alpha}$$
$$= \sup_{P_{\tilde{X}_1,\tilde{X}_2}} \sum_{y_1,y_2} P_{Y_1|X_1}(y_1|x_1')^{1-\beta}P_{Y_2|X_2}(y_2|x_2')^{1-\beta} \Big(\sum_{x_1,x_2} P_{\tilde{X}_1,\tilde{X}_2}(x_1,x_2)P_{Y_1|X_1}(y_1|x_1)^{\alpha}P_{Y_2|X_2}(y_2|x_2)^{\alpha}\Big)^{\beta/\alpha}. \tag{117}$$

Let $k(y_1)=\sum_{x_1} P_{\tilde{X}_1}(x_1)P_{Y_1|X_1}(y_1|x_1)^{\alpha}$, for all y_1, so that we can define a set of probability distributions over $\mathcal{X}_1$ as

$$P_{\hat{X}_1}(x_1|y_1)=\frac{P_{\tilde{X}_1}(x_1)P_{Y_1|X_1}(y_1|x_1)^{\alpha}}{k(y_1)}. \tag{118}$$

Thus, (117) is equal to

$$\sup_{P_{\tilde{X}_1,\tilde{X}_2}} \sum_{y_1,y_2} P_{Y_1|X_1}(y_1|x_1')^{1-\beta}P_{Y_2|X_2}(y_2|x_2')^{1-\beta} \Big[\sum_{x_1,x_2} k(y_1)P_{\hat{X}_1|Y_1}(x_1|y_1)P_{\tilde{X}_2|\tilde{X}_1}(x_2|x_1) P_{Y_2|X_2}(y_2|x_2)^{\alpha}\Big]^{\beta/\alpha} \tag{119}$$
$$\le \sup_{P_{\tilde{X}_1},P_{\tilde{X}_2|X_1}} \sum_{y_1} P_{Y_1|X_1}(y_1|x_1)^{1-\beta} \Big(\sum_{x_1} P_{\tilde{X}_1}(x_1)P_{Y_1|X_1}(y_1|x_1)^{\alpha}\Big)^{\frac{\beta}{\alpha}} \max_{\tilde{y}_1}\sum_{y_2} P_{Y_2|X_2}(y_2|x_2')^{1-\beta} \Big(\sum_{x_1,x_2} P_{\hat{X}_1|Y_1}(x_1|\tilde{y}_1)P_{\tilde{X}_2|\tilde{X}_1}(x_2|x_1)P_{Y_2|X_2}(y_2|x_2)^{\alpha}\Big)^{\beta/\alpha} \tag{120}$$
$$= \sup_{P_{\tilde{X}_1},P_{\tilde{X}_2|X_1}} \sum_{y_1} P_{Y_1|X_1}(y_1|x_1)^{1-\beta} \Big(\sum_{x_1} P_{\tilde{X}_1}(x_1)P_{Y_1|X_1}(y_1|x_1)^{\alpha}\Big)^{\frac{\beta}{\alpha}} \sum_{y_2} P_{Y_2|X_2}(y_2|x_2')^{1-\beta} \Big(\sum_{x_1,x_2} P_{\hat{X}_1|Y_1}(x_1|y_1^*)P_{\tilde{X}_2|\tilde{X}_1}(x_2|x_1)P_{Y_2|X_2}(y_2|x_2)^{\alpha}\Big)^{\beta/\alpha} \tag{121}$$

We now define

$$P_{\hat{X}_2}(x_2)=\sum_{x_1} P_{\hat{X}_1|Y_1}(x_1|y_1^*)P_{X_2|X_1}(x_2|x_1),$$

which is a probability distribution over $\mathcal{X}_2$. Then, (121) is equal to

$$\sup_{P_{\tilde{X}_1},\,P_{\hat{X}_2}} \sum_{y_1} P_{Y_1|X_1}(y_1|x_1')^{1-\beta}\Big(\sum_{x_1} P_{\tilde{X}_1}(x_1)P_{Y_1|X_1}(y_1|x_1)^{\alpha}\Big)^{\frac{\beta}{\alpha}} \times \sum_{y_2} P_{Y_2|X_2}(y_2|x_2')^{1-\beta}\Big(\sum_{x_2} P_{\hat{X}_2}(x_2)P_{Y_2|X_2}(y_2|x_2)^{\alpha}\Big)^{\frac{\beta}{\alpha}} \tag{122}$$
$$= \sup_{\substack{P_{\tilde{X}_i}\\ i\in 1,2}} \prod_{i=1}^{2}\Big(\sum_{y_i} P_{Y|X}(y_i|x_i')^{1-\beta} \times \Big(\sum_{x_i} P_{\tilde{X}_i}(x_i)P_{Y_i|X_i}(y_i|x_i)^{\alpha}\Big)^{\beta/\alpha}\Big). \tag{123}$$

This proves (115) as the lower bound part of (115) is trivial. Thus we have

$$\mathcal{L}_{\alpha,\beta}(X_1,X_2\to Y_1,Y_2)=\mathcal{L}_{\alpha,\beta}(X_1\to Y_1)+\mathcal{L}_{\alpha,\beta}(X_2\to Y_2). \tag{124}$$

Using (124) twice, we have

$$\mathcal{L}_{\alpha,\beta}(X^3\to Y^3) = \mathcal{L}_{\alpha,\beta}(X^2\to Y^2)+\mathcal{L}_{\alpha,\beta}(X_3\to Y_3) \tag{125}$$
$$= \mathcal{L}_{\alpha,\beta}(X_1\to Y_1)+\mathcal{L}_{\alpha,\beta}(X_2\to Y_2)+\mathcal{L}_{\alpha,\beta}(X_3\to Y_3). \tag{126}$$

Similarly, by repeated application of (124) $(n-1)$ times, we get (18).

Appendix C
Proof of Theorem 3

For $\alpha\in(1,\infty)$ and $\beta\in[1,\infty)$, we first bound $\mathcal{L}_{\alpha,\beta}(X\to Y|Z)$ from above and then, present an achievable scheme.

Upper Bound: Similarly to (49), the numerator and denominator of (19) become

$$\sum_{z,y} P_{Z,Y}(z,y)\left(\sum_u P_{U|Z,Y}(u|z,y)^{\alpha}\right)^{\beta/\alpha} \tag{127}$$

and

$$\sum_z P_Z(z)\left(\sum_u P_{U|Z}(u|z)^{\alpha}\right)^{\beta/\alpha}, \tag{128}$$

respectively. Thus, the logarithmic term in (19) reduces to

$$\log\frac{\sum_{z,y} P_{Z,Y}(z,y)\left(\sum_u P_{U|Z,Y}(u|z,y)^{\alpha}\right)^{\beta/\alpha}}{\sum_z P_Z(z)\left(\sum_u P_{U|Z}(u|z)^{\alpha}\right)^{\beta/\alpha}} \tag{129}$$
$$=\log\frac{\sum_z P_Z(z)\sum_y P_{Y|Z}(y|z)\left(\sum_u P_{U|Z,Y}(u|z,y)^{\alpha}\right)^{\beta/\alpha}}{\sum_z P_Z(z)\left(\sum_u P_{U|Z}(u|z)^{\alpha}\right)^{\beta/\alpha}} \tag{130}$$
$$\le \log\max_z \frac{\sum_y P_{Y|Z}(y|z)\left(\sum_u P_{U|Z,Y}(u|z,y)^{\alpha}\right)^{\beta/\alpha}}{\left(\sum_u P_{U|Z}(u|z)^{\alpha}\right)^{\beta/\alpha}} \tag{131}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \max_z \log \frac{\sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\sum_u P_{Y,U|Z}(y,u|z)^\alpha \right)^{\beta/\alpha}}{\left(\sum_u P_{U|Z}(u|z)^\alpha \right)^{\beta/\alpha}} \tag{132}$$

where (131) follows from the fact that for any non-negative a_i and b_i, we have $\frac{\sum_i a_i}{\sum_i b_i} \leq \max_i \frac{a_i}{b_i}$. Moreover, we have

$$P_{Y,U|Z}(y,u|z)^\alpha = P_{U|Z}(u|z)^\alpha P_{Y|U,Z}(y|u,z)^\alpha \tag{133}$$

and

$$P_{Y|U,Z}(y|u,z)^\alpha = \left(\sum_x P_{X|U,Z}(x|u,z) P_{Y|X,Z}(y|x,z) \right)^\alpha \tag{134}$$

$$\leq \sum_x P_{X|U,Z}(x|u,z) P_{Y|X,Z}(y|x,z)^\alpha \tag{135}$$

where the equality follows because $U - X - Y|Z$ holds, and the inequality follows from applying Jensen's inequality to the convex function $f: x \to x^p$ $(x \geq 0,\ p > 1)$. Applying (135) to (132), we may bound $\mathcal{L}_{\alpha,\beta}(X \to Y|Z)$ from above by

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z)$$

$$\leq \sup_{P_{X|Z}} \sup_{U \to X \to Y|Z} \max_z \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\frac{\sum_x P_{Y|X,Z}(y|x,z)^\alpha \sum_u P_{U|Z}(u|z)^\alpha P_{X|U,Z}(x|u,z)}{\sum_u P_{U|Z}(u|z)^\alpha} \right)^{\frac{\beta}{\alpha}} \tag{136}$$

$$\leq \max_z \sup_{P_{X|Z=z}} \sup_{\substack{P_{\tilde{X}|Z=z} \\ \ll P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z)^\alpha P_{\tilde{X}|Z=z}(x) \right)^{\frac{\beta}{\alpha}} \tag{137}$$

where

$$P_{\tilde{X}|Z=z}(x) = \frac{\sum_u P_{U|Z}(u|z)^\alpha P_{X|U,Z}(x|u,z)}{\sum_u P_{U|Z}(u|z)^\alpha}. \tag{138}$$

Lower Bound: For this proof, we use the expression in (129) as well as shattering method. For a given conditional distribution $P_{Y|X,Z}$, let

$$z^* = \arg\max_z \sup_{P_{X|Z=z}} \sup_{\substack{P_{\tilde{X}|Z=z} \\ \ll P_{X|Z=z}}} \sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z=z}(x) P_{Y|X,Z}(y|x,z)^\alpha \right)^{\frac{\beta}{\alpha}} \tag{139}$$

and

$$\mathcal{X}_{z^*} = \{x \in \mathcal{X} : P_{X,Z}(x,z^*) > 0\}. \tag{140}$$

Consider a random variable U whose alphabet consists of several disjoint subsets. For all $x \in \mathcal{X}_{z^*}$, let $\mathcal{U}_{x,z^*}$ be disjoint, finite sets. Moreover, let $\mathcal{U}_0$ be a finite set (disjoint from those above) such that $\mathcal{U} = \mathcal{U}_0 \cup \bigcup_{x \in \mathcal{X}_{z^*}} \mathcal{U}_{x,z^*}$. We now define the conditional distribution $P_{U|X,Z}$ as

$$P_{U|X,Z}(u|x,z) = \begin{cases} \frac{1}{|\mathcal{U}_{x,z^*}|}, & z = z^*, u \in \mathcal{U}_{x,z^*} \\ \frac{1}{|\mathcal{U}_0|}, & z \neq z^*, u \in \mathcal{U}_0 \\ 0, & \text{otherwise.} \end{cases} \tag{141}$$

So the numerator of (129) reduces to

$$\sum_{z,y} P_{Z,Y}(z,y) \left(\sum_u P_{U|Z,Y}(u|z,y)^\alpha \right)^{\beta/\alpha} \tag{142}$$

$$= \sum_{z \neq z^*, y} P_{Z,Y}(z,y) \left(\sum_u P_{U|Z,Y}(u|z,y)^\alpha \right)^{\beta/\alpha} + P_Z(z^*) \sum_y P_{Y|Z}(y|z^*)^{1-\beta} \left(\sum_u P_{U,Y|Z}(u,y|z^*)^\alpha \right)^{\beta/\alpha}. \tag{143}$$

where

$$\left(\sum_u P_{U|Z,Y}(u|z,y)^\alpha \right)^{\beta/\alpha} \tag{144}$$

$$= \left(\sum_u \left(\sum_x P_{X|Z,Y}(x|z,y) P_{U|Z,X}(u|z,x) \right)^\alpha \right)^{\beta/\alpha} \tag{145}$$

$$= \left(|\mathcal{U}_0| \left(\sum_x P_{X|Z,Y}(x|z,y) \frac{1}{|\mathcal{U}_0|} \right)^\alpha \right)^{\beta/\alpha} \tag{146}$$

$$= \left(|\mathcal{U}_0|^{1-\alpha} \right)^{\beta/\alpha} \tag{147}$$

and

$$\left(\sum_u P_{U,Y|Z}(u,y|z^*)^\alpha \right)^{\beta/\alpha} \tag{148}$$

$$= \left(\sum_u \left[\sum_{x'} P_{X|Z}(x'|z^*) \times P_{U|X,Z}(u|x',z^*) P_{Y|X,Z}(y|x',z^*) \right]^\alpha \right)^{\beta/\alpha} \tag{149}$$

$$= \left(\sum_x \sum_{u \in \mathcal{U}_{x,z^*}} \left[\sum_{x'} P_{X|Z}(x'|z^*) \times P_{U|X,Z}(u|x',z^*) P_{Y|X,Z}(y|x',z^*) \right]^\alpha \right)^{\beta/\alpha} \tag{150}$$

$$= \left(\sum_x |\mathcal{U}_{x,z^*}| \left[P_{X|Z}(x|z^*) \times \frac{1}{|\mathcal{U}_{x,z^*}|} P_{Y|X,Z}(y|x,z^*) \right]^\alpha \right)^{\frac{\beta}{\alpha}} \tag{151}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \left(\sum_x |\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha \; P_{Y|X,Z}(y|x,z^*)^\alpha \right)^{\beta/\alpha}. \tag{152}$$

Here (145) and (149) follow because $U - X - Y|Z$ holds. Applying (147) and (152) to (143), the numerator of (129) becomes

$$\frac{1-P_Z(z^*)}{|\mathcal{U}_0|^{(1-\frac{1}{\alpha})\beta}} + P_Z(z^*) \sum_y P_{Y|Z}(y|z^*)^{1-\beta} \left(\sum_x |\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha \; P_{Y|X,Z}(y|x,z^*)^\alpha \right)^{\beta/\alpha}. \tag{153}$$

Similarly, the denominator of (129) becomes

$$\frac{1-P_Z(z^*)}{|\mathcal{U}_0|^{(1-\frac{1}{\alpha})\beta}} + P_Z(z^*) \left(\sum_x |\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha \right)^{\beta/\alpha}. \tag{154}$$

Note that for $\alpha \in (1,\infty)$ and $\beta \in [1,\infty)$, $\frac{1-P_Z(z^*)}{|\mathcal{U}_0|^{(1-\frac{1}{\alpha})\beta}} \to 0$ as $|\mathcal{U}_0| \to \infty$. So we may bound the conditional maximal (α,β)-leakage from below by

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) \geq \sup_{P_{X|Z=z^*}} \sup_{\mathcal{U}_{x,z^*}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z^*)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z^*)^\alpha \frac{|\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha}{\sum_x |\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha} \right)^{\frac{\beta}{\alpha}} \tag{155}$$

$$= \sup_{P_{X|Z=z^*}} \sup_{P_{\tilde{X}|Z=z^*} \ll P_{X|Z=z^*}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z^*)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z^*)^\alpha \times P_{\tilde{X}|Z=z^*}(x) \right)^{\frac{\beta}{\alpha}}, \tag{156}$$

where here

$$P_{\tilde{X}|Z=z^*}(x) = \frac{|\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha}{\sum_x |\mathcal{U}_{x,z^*}|^{1-\alpha} P_{X|Z}(x|z^*)^\alpha} \tag{157}$$

and we have used the fact that any distribution $P_{\tilde{X}|Z=z^*}(x)$ can be reached with appropriate choice of $|\mathcal{U}_{x,z^*}|$. Recalling the definition of z^* from (139), we may re-write (156) as

$$\max_z \sup_{P_{X|Z=z}} \sup_{\substack{P_{\tilde{X}|Z=z} \\ \ll P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z)^\alpha \; P_{\tilde{X}|Z=z}(x) \right)^{\frac{\beta}{\alpha}} \tag{158}$$

Therefore, combining (137) and (158), we have

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) = \max_z \sup_{P_{X|Z=z}} \sup_{\substack{P_{\tilde{X}|Z=z} \ll \\ P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|Z}(y|z)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z)^\alpha P_{\tilde{X}|Z=z}(x) \right)^{\frac{\beta}{\alpha}}. \tag{159}$$

Since the choice of $P_{X|Z=z}$ only impacts $P_{Y|Z}$, and the supremum of a convex function is attained at an extreme point, we may simplify (159) as follows.

$$\max_z \max_{x'} \sup_{\substack{P_{\tilde{X}|Z=z} \ll \\ P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X,Z}(y|x',z)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z)^\alpha P_{\tilde{X}|Z=z}(x) \right)^{\frac{\beta}{\alpha}}. \tag{160}$$

Appendix D
Proof of Theorem 4

From (20), we have

$$\mathcal{L}_{\alpha,\beta}(X \to Y|Z) = \max_z \max_{x'} \sup_{\substack{P_{\tilde{X}} \ll \\ P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X,Z}(y|x',z)^{1-\beta} \left(\sum_x P_{Y|X,Z}(y|x,z)^\alpha P_{\tilde{X}}(x) \right)^{\frac{\beta}{\alpha}} \tag{161}$$

$$= \max_z \max_{x'} \sup_{\substack{P_{\tilde{X}} \ll \\ P_{X|Z=z}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{Y|X}(y|x)^\alpha P_{\tilde{X}}(x) \right)^{\frac{\beta}{\alpha}} \tag{162}$$

$$\leq \max_{x'} \sup_{P_{\tilde{X}} \ll P_X} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{Y|X}(y|x)^\alpha P_{\tilde{X}}(x) \right)^{\frac{\beta}{\alpha}} \tag{163}$$

$$= \mathcal{L}_{\alpha,\beta}(X \to Y),$$

where (162) follows because the Markov chain $Z - X - Y$ holds, and (163) follows from the fact that for any z, the support of $P_{X|Z=z}$ is a subset of the support of P_X. The equality is achieved if for some $z \in \text{supp}(Z)$, $\text{supp}(X) = \text{supp}(X|Z=z)$.

Appendix E
Proof of Theorem 5

We have

$$\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2|Z) = \max_{z,x'} \sup_{P_{\tilde{X}|Z}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_{y_1,y_2} P_{Y_1,Y_2|X,Z}(y_1,y_2|x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1,Y_2|X,Z}(y_1,y_2|x,z)^\alpha \right)^{\beta/\alpha}. \tag{164}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

We reduce the argument of the logarithm in (164) as follows.

$$\sum_{y_1,y_2} P_{Y_1,Y_2|X,Z}(y_1,y_2|x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z)\ P_{Y_1,Y_2|X,Z}(y_1,y_2|x,z)^{\alpha}\right)^{\beta/\alpha} \tag{165}$$

$$= \sum_{y_1,y_2} P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} P_{Y_2|Y_1,X,Z}(y_2|y_1,x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha} \times P_{Y_2|Y_1,X,Z}(y_2|y_1,x,z)^{\alpha}\right)^{\beta/\alpha}. \tag{166}$$

Let $K(y_1,z) = \sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}$, for all $y_1 \in \mathcal{Y}_1$ and $z \in \mathcal{Z}$. So, we can construct a set of distributions over $\mathcal{X}$ as

$$P_{\bar{X}|Y_1,Z}(x|y_1,z) = \frac{P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}}{K(y_1,z)}. \tag{167}$$

Thus, we may rewrite the expression in (166) as

$$\sum_{y_1,y_2} P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} P_{Y_2|Y_1,X,Z}(y_2|y_1,x',z)^{1-\beta} \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1,z)\ K(y_1,z) \times P_{Y_2|Y_1,X,Z}(y_2|y_1,x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \tag{168}$$

$$= \sum_{y_1,y_2} \Bigg[P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} P_{Y_2|Y_1,X,Z}(y_2|y_1,x',z)^{1-\beta} \times \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \times \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1,z)\ P_{Y_2|Y_1,X,Z}(y_2|y_1,x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \Bigg] \tag{169}$$

$$= \sum_{y_1} \Bigg[P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z) \times P_{Y_1|X,Z}(y_1|x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \sum_{y_2} P_{Y_2|Y_1,X,Z}(y_2|y_1,x',z)^{1-\beta} \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1,z)\ P_{Y_2|Y_1,X,Z}(y_2|y_1,x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \Bigg] \tag{170}$$

$$\leq \Bigg[\sum_{y_1} P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \Bigg] \Bigg[\max_{y_1' \in \mathcal{Y}} \sum_{y_2} P_{Y_2|Y_1,X,Z}(y_2|y_1',x',z)^{1-\beta} \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1',z) P_{Y_2|Y_1,X,Z}(y_2|y_1',x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \Bigg]. \tag{171}$$

Applying (171) to (164), we have

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y_1, Y_2|Z) \\
&\leq \max_{z,x'} \sup_{P_{\tilde{X}|Z}} \frac{\alpha}{(\alpha-1)\beta} \Bigg[\log \sum_{y_1} P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} \times \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \\
&\quad + \max_{y_1'} \log \sum_{y_2} P_{Y_2|Y_1,X,Z}(y_2|y_1',x',z)^{1-\beta} \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1',z) P_{Y_2|Y_1,X,Z}(y_2|y_1',x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} \Bigg] && (172) \\
&\leq \max_{z,x'} \sup_{P_{\tilde{X}|Z}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_{y_1} P_{Y_1|X,Z}(y_1|x',z)^{1-\beta} \left(\sum_x P_{\tilde{X}|Z}(x|z) P_{Y_1|X,Z}(y_1|x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} + \max_{y_1',z,x'} \sup_{P_{\bar{X}|Y_1,Z}} \\
&\quad \frac{\alpha}{(\alpha-1)\beta} \log \sum_{y_2} P_{Y_2|Y_1,X,Z}(y_2|y_1',x',z)^{1-\beta} \left(\sum_x P_{\bar{X}|Y_1,Z}(x|y_1',z) P_{Y_2|Y_1,X,Z}(y_2|y_1',x,z)^{\alpha}\right)^{\frac{\beta}{\alpha}} && (173) \\
&= \mathcal{L}_{\alpha,\beta}(X \to Y_1|Z) + \mathcal{L}_{\alpha,\beta}(X \to Y_2|Y_1,Z). && (174)
\end{aligned}$$

Appendix F
Proof of Proposition 1

For $\alpha \leq \beta$, maximal (α,β)-leakage simplifies to

$$\begin{aligned}
&\mathcal{L}_{\alpha,\beta}(X \to Y) \\
&= \max_{x'} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha}\right)^{\beta/\alpha} && (175) \\
&= \max_{x'} \max_x \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} P_{Y|X}(y|x)^{\beta}, && (176)
\end{aligned}$$

where (176) follows because the argument of the logarithm in (175) is convex in $P_{\tilde{X}}$ and so the supremum is attained at an extreme point. This quantity represents a *scaled version of LRDP of order* β which is exactly equal to LRDP for $\alpha = \beta$. We now take the limits of maximal α,β-leakage in (14) as $\alpha \to \infty$ and $\beta \to \infty$. We have

$$\lim_{\beta\to\infty} \lim_{\alpha\to\infty} \mathcal{L}_{\alpha,\beta}(X \to Y) = \lim_{\beta\to\infty} \mathcal{L}_{\beta}(X \to Y), \tag{177}$$

We first bound $\lim_{\beta\to\infty} \mathcal{L}_{\beta}(X \to Y)$ from above as follows.

$$\begin{aligned}
&\mathcal{L}_{\beta}(X \to Y) \\
&= \max_{x'} \frac{1}{\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^{\beta} && (178) \\
&= \max_{x'} \frac{1}{\beta} \log \sum_y P_{Y|X}(y|x') \left(\frac{\max_x P_{Y|X}(y|x)}{P_{Y|X}(y|x')}\right)^{\beta} && (179)
\end{aligned}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$\leq \max_{x'} \frac{1}{\beta} \log \sum_y P_{Y|X}(y|x') \max_y \left(\frac{\max_x P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right)^\beta \tag{180}$$

$$= \max_{x'} \frac{1}{\beta} \log \max_y \left(\frac{\max_x P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right)^\beta \sum_y P_{Y|X}(y|x') \tag{181}$$

$$= \max_{x',y} \log \left(\frac{\max_x P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right) \tag{182}$$

$$= \max_{x',y,x} \log \left(\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right) \tag{183}$$

As the next step, we provide an achievable scheme. Let $x^*, y^*, x'^* = \arg\max_{x,y,x'} \frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')}$, we have

$$\mathcal{L}_\beta(X \to Y)$$

$$= \max_{x'} \frac{1}{\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^\beta \tag{184}$$

$$\geq \max_{x'} \frac{1}{\beta} \log \max_y \left[P_{Y|X}(y|x')^{1-\beta} \max_x P_{Y|X}(y|x)^\beta \right] \tag{185}$$

$$= \frac{1}{\beta} \log \max_{y,x,x'} \left(\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right)^\beta P_{Y|X}(y|x') \tag{186}$$

$$\geq \frac{1}{\beta} \log \left(\frac{P_{Y|X}(y^*|x^*)}{P_{Y|X}(y^*|x'^*)} \right)^\beta P_{Y|X}(y^*|x'^*) \tag{187}$$

$$= \log \frac{P_{Y|X}(y^*|x^*)}{P_{Y|X}(y^*|x'^*)} + \frac{1}{\beta} \log P_{Y|X}(y^*|x'^*), \tag{188}$$

So

$$\lim_{\beta\to\infty} \mathcal{L}_\beta(X \to Y) \geq \log \frac{P_{Y|X}(y^*|x^*)}{P_{Y|X}(y^*|x'^*)} = \max_{x,y,x'} \log \frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')}. \tag{189}$$

Combining (183) and (189) gives

$$\lim_{\beta\to\infty} \mathcal{L}_\beta(X \to Y) = \max_{x,y,x'} \log \frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')}, \tag{190}$$

which is LDP.

Appendix G
Proof of Proposition 3

Applying Theorem 3, for finite alphabets, vector maximal (α, β)-leakage defined in (25) simplifies to

$$\mathcal{L}^{\text{vec}}_{\alpha,\beta}(X^n \to Y) = \max_{i,x_{-i},x'_i} \sup_{P_{\tilde{X}_i|X_{-i}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X_i,X_{-i}}(y|x'_i, x_{-i})^{1-\beta} \left(\sum_{x_i} P_{Y|X_i,X_{-i}}(y|x_i, x_{-i})^\alpha P_{\tilde{X}_i|X_{-i}}(x_i|x_{-i}) \right)^{\frac{\beta}{\alpha}}, \tag{191}$$

where $P_{\tilde{X}_i|X_{-i}}$ is a distribution on the support of $P_{X_i|X_{-i}}$. The expression of vector maximal α-leakage in (27) can be readily obtained by setting β equal to 1. For $\alpha \leq \beta$, applying Proposition 2, we can simplify the above expression to

$$\mathcal{L}^{\text{vec}}_{\alpha\leq\beta}(X^n \to Y) = \max_{i,x_{-i},x'_i,x_i} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X_i,X_{-i}}(y|x'_i, x_{-i})^{1-\beta} P_{Y|X_i,X_{-i}}(y|x_i, x_{-i})^\beta. \tag{192}$$

Note that (x'_i, x_{-i}) and (x_i, x_{-i}) can be considered as two datasets which differ only in the ith entries. So, the maximums over x_i, x'_i, and x_{-i} explore neighboring datasets differing in ith entries, and the maximum across all i ensures the consideration of all possible neighboring datasets. Thus, the above expression may be rewritten to the following form:

$$\max_{x^n \sim x'^n} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X^n}(y|x'^n)^{1-\beta} P_{Y|X^n}(y|x^n)^\beta, \tag{193}$$

which is a scaled RDP of order β with the scaling factor of $\frac{\alpha(\beta-1)}{(\alpha-1)\beta}$. Moreover, when $\alpha = \beta$, this quantity is exactly equal to RDP of order $\alpha = \beta$ which in turn recovers DP as $\alpha = \beta \to \infty$. For $\alpha \to \infty$ and an arbitrary β, applying Proposition 2, we get the expression of vector maximal Rényi leakage.

Appendix H
Proof of Lemma 1

We first prove the expression (32) which provides a still other representation of the leakage measure.

Consider any $\gamma \in (-\infty, 0] \cup [1, \infty)$, and any constants $C(y)$ for $y \in \mathcal{Y}$. Furthermore, consider the optimization problem

$$\inf_{Q_Y} \sum_y C(y) Q_Y(y)^\gamma. \tag{194}$$

γ is in the range where (194) is convex in Q_Y, so it is solved by setting the derivative of $Q_Y(y)$ to a constant:

$$\nu = \frac{\partial}{\partial Q_Y(y)} \sum_y C(y) Q_Y(y)^\gamma = C(y)\ \gamma\ Q_Y(y)^{\gamma-1}. \tag{195}$$

We can see that the optimal choice is therefore

$$Q_Y(y) = \frac{C(y)^{1/(1-\gamma)}}{\sum_{y'} C(y')^{1/(1-\gamma)}}. \tag{196}$$

Thus (194) becomes

$$\frac{\sum_y C(y) C(y)^{\gamma/(1-\gamma)}}{\left(\sum_{y'} C(y')^{1/(1-\gamma)}\right)^\gamma} = \left(\sum_y C(y)^{1/(1-\gamma)} \right)^{1-\gamma}. \tag{197}$$

In our case, we have $\gamma = \frac{1-\alpha}{\tau} < 0$, and

$$C(y) = \sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^\alpha P_{Y|X}(y|x')^{(1-\frac{1}{\tau})(1-\alpha)}. \tag{198}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

Applying the result in (197) to our case, we find that (32) is equal to

$$\max_{x'} \sup_{P_{\tilde{X}}} \frac{1}{\alpha-1} \log \left[\sum_y \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times P_{Y|X}(y|x')^{(1-\frac{1}{\tau})(1-\alpha)} \right)^{\frac{\tau}{\tau+\alpha-1}} \right]^{\frac{\tau+\alpha-1}{\tau}} \tag{199}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} \left(\frac{1}{\alpha-1} + \frac{1}{\tau} \right) \log \sum_y P_{Y|X}(y|x')^{\frac{(\tau-1)(1-\alpha)}{\tau+\alpha-1}} \times \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \right)^{\frac{\tau}{\tau+\alpha-1}} \tag{200}$$

which is precisely (31).

Moreover, we claim that maximal (α, τ)-leakage is non-decreasing in τ and α for a fixed α and τ, respectively. Since β is increasing in τ, the first claim, that the measure is non-decreasing in τ, is equivalent to it being non-decreasing in β, which we have already proved in Appendix B. Given the expression (32), we prove that $\mathcal{L}_{\alpha,\tau}(X \to Y)$ is non-decreasing in α for a fixed τ as follows. We may write the objective function in (32) as

$$\frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \times \left(\frac{P_{Y|X}(y|x)}{Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}} \right)^{\alpha-1}. \tag{201}$$

This expression is non-decreasing in α due to the fact that, for any distribution P_Z, and any constants $C(z)$,

$$\frac{1}{\alpha-1} \log \sum_z P_Z(z) C(z)^{\alpha-1} \tag{202}$$

is non-decreasing in α for $\alpha > 1$.

Appendix I
Proof of Proposition 4

For a fixed τ, we have

$$\lim_{\alpha\to 1} \mathcal{L}_{\alpha,\tau}(X \to Y)$$

$$= \lim_{\alpha\to 1} \max_{x'} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{203}$$

$$= \max_{x'} \lim_{\alpha\to 1} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{204}$$

$$= \max_{x'} \inf_{\alpha} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{205}$$

$$= \max_{x'} \inf_{\alpha} \inf_{Q_Y} \sup_{P_{\tilde{X}}} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{206}$$

$$= \max_{x'} \inf_{Q_Y} \inf_{\alpha} \sup_{P_{\tilde{X}}} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{207}$$

$$= \max_{x'} \inf_{Q_Y} \lim_{\alpha\to 1} \sup_{P_{\tilde{X}}} \frac{1}{\alpha-1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{208}$$

$$= \max_{x'} \inf_{Q_Y} \lim_{\alpha\to 1} \max_{x} \frac{1}{\alpha-1} \log \sum_{y} P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{209}$$

$$= \max_{x'} \inf_{Q_Y} \max_{x} \lim_{\alpha\to 1} \frac{1}{\alpha-1} \log \sum_{y} P_{Y|X}(y|x)^{\alpha} \times \left(Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}} \right)^{1-\alpha} \tag{210}$$

$$= \max_{x'} \inf_{Q_Y} \max_{x} \sum_{y} P_{Y|X}(y|x) \log \frac{P_{Y|X}(y|x)}{Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}} \tag{211}$$

$$= \max_{x'} \inf_{Q_Y} \sup_{P_{\tilde{X}}} \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \times \log \frac{P_{Y|X}(y|x)}{Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}} \tag{212}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \times \log \frac{P_{Y|X}(y|x)}{Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}} \tag{213}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} \inf_{Q_Y} \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \times \log \left(\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right)^{1-\frac{1}{\tau}} \left(\frac{P_{Y|X}(y|x)}{Q_Y(y)} \right)^{\frac{1}{\tau}} \tag{214}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} \inf_{Q_Y} (1-\frac{1}{\tau}) \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \times \log \left(\frac{P_{Y|X}(y|x)}{P_{Y|X}(y|x')} \right) + \frac{1}{\tau} \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x) \log \left(\frac{P_{Y|X}(y|x)}{Q_Y(y)} \right) \tag{215}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} \left[(1-\frac{1}{\tau}) D_{KL} \left(P_{Y|X}(y|x) \| P_{Y|X}(y|x') | P_{\tilde{X}}(x) \right) + \frac{1}{\tau} \inf_{Q_Y} D_{KL}(P_{\tilde{X}}(x) P_{Y|X}(y|x) \| P_{\tilde{X}}(x) Q_Y(y)) \right] \tag{216}$$

$$= \max_{x'} \sup_{P_{\tilde{X}}} (1-\frac{1}{\tau}) D_{KL} \left(P_{Y|X}(y|x) \| P_{Y|X}(y|x') | P_{\tilde{X}}(x) \right) + \frac{1}{\tau} I(\tilde{X}; Y), \tag{217}$$

where

- (205) and (208) follow because the objective function is non-decreasing in α,
- (206) follows because the quantity inside the log is linear (and thus concave) in $P_{\tilde{X}}$ and convex in Q_Y,

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

- (209) follows because the quantity inside the log is linear in $P_{\tilde{X}}$ and so supremum is attained at a corner point,
- (211) follows from L'Hopital's rule,
- (212) follows because the objective function in (212) is linear in $P_{\tilde{X}}$ and so the sup is attained at a corner point,
- (213) follows because the objective is linear (thus concave) in $P_{\tilde{X}}$ and convex in Q_Y.

Appendix J
Proof of Theorem 6

We first prove the continuity of maximal (α, τ)-leakage, and following that, we demonstrate the continuity of MαbeL. In our analysis, we employ the extended real number line.

A. Continuity of Maximal (α, τ)-Leakage

Let

$$\tau_\epsilon^-(\tau_0) = \begin{cases} \tau_0 - \epsilon & \text{if } \tau_0 \in (1, \infty) \\ \frac{1}{\epsilon} & \text{if } \tau_0 = \infty \\ 1 & \text{if } \tau_0 = 1, \end{cases} \tag{218}$$

$$\tau_\epsilon^+(\tau_0) = \begin{cases} \tau_0 + \epsilon & \text{if } \tau_0 \in [1, \infty) \\ \infty & \text{if } \tau_0 = \infty, \end{cases} \tag{219}$$

$$\alpha_\epsilon^-(\alpha_0) = \begin{cases} \alpha_0 - \epsilon & \text{if } \alpha_0 \in (1, \infty) \\ \frac{1}{\epsilon} & \text{if } \alpha_0 = \infty \\ 1 & \text{if } \alpha_0 = 1, \end{cases} \tag{220}$$

and

$$\alpha_\epsilon^+(\alpha_0) = \begin{cases} \alpha_0 + \epsilon & \text{if } \alpha_0 \in [1, \infty) \\ \infty & \text{if } \alpha_0 = \infty. \end{cases} \tag{221}$$

To prove the continuity of maximal (α, τ)-leakage at $(\alpha_0, \tau_0) \in [1, \infty] \times [1, \infty]$, we define a rectangular region characterized by its corners at $(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0))$, $(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^+(\tau_0))$, $(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^-(\tau_0))$, and $(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0))$, with the point (α_0, τ_0) lying inside or on the borders of this region, and we show that

$$\begin{aligned} &\lim_{\epsilon \to 0} \inf_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \\ &= \lim_{\epsilon \to 0} \sup_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \qquad (222) \\ &= \mathcal{L}_{\alpha_0,\tau_0}(X \to Y). \qquad (223) \end{aligned}$$

Note that the rectangular region converges to the point (α_0, τ_0) as $\epsilon \to 0$. We recall that

$$\begin{cases} \mathcal{L}_{\alpha=1,\tau}(X \to Y)) = \tau\text{-Shannon leakage} \\ \mathcal{L}_{\alpha=\infty,\tau}(X \to Y) = \text{Maximal Rényi leakage of order } \tau \\ \mathcal{L}_{\alpha,\tau=\infty}(X \to Y) = \mathcal{L}_\alpha^{\text{LRDP}}(X \to Y) \\ \mathcal{L}_{\alpha=\infty,\tau=\infty}(X \to Y) = \mathcal{L}^{\text{LDP}}(X \to Y). \end{cases} \tag{224}$$

Lower bound: For $(\alpha, \tau) \in (1, \infty) \times [1, \infty)$, we have

$$\mathcal{L}_{\alpha,\tau}(X \to Y) = \max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha, \tau), \tag{225}$$

where

$$Q_{x', P_{\tilde{X}}}(\alpha, \tau) = \left(\frac{1}{\alpha - 1} + \frac{1}{\tau}\right) \log \sum_y P_{Y|X}(y|x')^{\frac{(\tau-1)(1-\alpha)}{\tau+\alpha-1}} \times \left(\sum_x P_{\tilde{X}}(x) P_{Y|X}(y|x)^\alpha\right)^{\frac{\tau}{\tau+\alpha-1}}. \tag{226}$$

$Q_{x', P_{\tilde{X}}}(\alpha, \tau)$ is continuous in (α, τ), for all $(\alpha, \tau) \in (1, \infty) \times [1, \infty)$, and it may be defined by its continuous extension at $\alpha = \infty$, $\tau = \infty$, or $\alpha = 1$, (227), as shown at the bottom of the next page. We know that (225) holds for $(\alpha, \tau) \in (1, \infty) \times [1, \infty)$. Now we show that it also holds for $(\alpha, \tau) \in [1, \infty]^2 \setminus (1, \infty) \times [1, \infty)$. Employing (224) and (227), for $(\alpha, \tau) \in \{1, \infty\} \times [1, \infty]$, we can see that

$$\max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha, \tau) = \mathcal{L}_{\alpha,\tau}(X \to Y). \tag{228}$$

For $\alpha \in (1, \infty)$ and $\tau = \infty$, we also have

$$\begin{aligned} &\max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha, \tau = \infty) \\ &= \max_{x'} \sup_{P_{\tilde{X}}} \frac{1}{\alpha - 1} \log \sum_{x,y} P_{\tilde{X}}(x) P_{Y|X}(y|x')^{1-\alpha} P_{Y|X}(y|x)^\alpha \qquad (229) \\ &= \max_{x'} \max_x \frac{1}{\alpha - 1} \log \sum_y P_{Y|X}(y|x')^{1-\alpha} P_{Y|X}(y|x)^\alpha \qquad (230) \\ &= \mathcal{L}_{\alpha,\tau=\infty}(X \to Y), \qquad (231) \end{aligned}$$

where (230) follows because the quantity inside the logarithm is linear in $P_{\tilde{X}}$ and so the supremum is achieved at an endpoint.

For $(\alpha_0, \tau_0) \in [1, \infty] \times [1, \infty]$, we have

$$\begin{aligned} &\lim_{\epsilon \to 0} \inf_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \qquad (232) \\ &= \lim_{\epsilon \to 0} \mathcal{L}_{\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)}(X \to Y) \qquad (233) \\ &= \lim_{\epsilon \to 0} \max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)) \qquad (234) \\ &= \max_{x'} \lim_{\epsilon \to 0} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)) \qquad (235) \\ &= \max_{x'} \sup_{\epsilon > 0} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)) \qquad (236) \\ &= \max_{x'} \sup_{P_{\tilde{X}}} \sup_{\epsilon > 0} Q_{x', P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)) \qquad (237) \\ &= \max_{x'} \sup_{P_{\tilde{X}}} \lim_{\epsilon \to 0} Q_{x', P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0), \tau_\epsilon^-(\tau_0)) \qquad (238) \\ &= \max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha_0^-(\alpha_0), \tau_0^-(\tau_0)) \qquad (239) \\ &= \max_{x'} \sup_{P_{\tilde{X}}} Q_{x', P_{\tilde{X}}}(\alpha_0, \tau_0) \qquad (240) \\ &= \mathcal{L}_{\alpha_0,\tau_0}(X \to Y) \qquad (241) \end{aligned}$$

where (233) follows because $\mathcal{L}_{\alpha,\tau}(X \to Y)$ is non-decreasing in α and τ. (236) and (238) follow because $Q_{x', P_{\tilde{X}}}(\alpha, \tau)$ is non-decreasing in α and τ for a fixed τ and α, respectively. Moreover, $\alpha_\epsilon^-(\alpha_0)$ and $\tau_\epsilon^-(\tau_0)$ are non-increasing in ϵ for

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

a fixed α_0 and τ_0, respectively. The equality (239) follows because $Q_{x',P_{\tilde{X}}}(\alpha_\epsilon^-(\alpha_0),\tau_\epsilon^-(\tau_0))$ is continuous in ϵ.

Upper Bound: For $(\alpha,\tau)\in(1,\infty)\times[1,\infty)$, consider the expression of $\mathcal{L}_{\alpha,\tau}(X\to Y)$ in (32):

$$\begin{aligned}
&\mathcal{L}_{\alpha,\tau}(X\to Y)\\
&=\max_{x'}\sup_{P_{\tilde{X}}}\inf_{Q_Y}\frac{1}{\alpha-1}\log\sum_{x,y}P_{\tilde{X}}(x)P_{Y|X}(y|x)^{\alpha}\\
&\quad\times\left(Q_Y(y)^{\frac{1}{\tau}}P_{Y|X}(y|x')^{1-\frac{1}{\tau}}\right)^{1-\alpha} &(242)\\
&=\max_{x'}\inf_{Q_Y}\sup_{P_{\tilde{X}}}\frac{1}{\alpha-1}\log\sum_{x,y}P_{\tilde{X}}(x)P_{Y|X}(y|x)^{\alpha}\\
&\quad\times\left(Q_Y(y)^{\frac{1}{\tau}}P_{Y|X}(y|x')^{1-\frac{1}{\tau}}\right)^{1-\alpha} &(243)\\
&=\max_{x'}\inf_{Q_Y}\max_{x}\frac{1}{\alpha-1}\log\sum_{y}P_{Y|X}(y|x)^{\alpha}\\
&\quad\times\left(Q_Y(y)^{\frac{1}{\tau}}P_{Y|X}(y|x')^{1-\frac{1}{\tau}}\right)^{1-\alpha} &(244)
\end{aligned}$$

where (243) follows because the quantity inside the logarithm is convex in Q_Y and linear (so concave) in $P_{\tilde{X}}$, and (244) follows because the quantity inside the logarithm is linear in $P_{\tilde{X}}$ and so the supremum is achieved at an endpoint. Consider the objective in (244):

$$\begin{aligned}
&f_{x',Q_Y,x}(\alpha,\tau)\\
&=\frac{1}{\alpha-1}\log\sum_{y}P_{Y|X}(y|x)^{\alpha}\left(Q_Y(y)^{\frac{1}{\tau}}P_{Y|X}(y|x')^{1-\frac{1}{\tau}}\right)^{1-\alpha} &(245)\\
&=\log\left[\sum_{y}P_{Y|X}(y|x)\left(P_{Y|X}(y|x)\,Q_Y(y)^{-\frac{1}{\tau}}\right.\right.\\
&\quad\left.\left.\times P_{Y|X}(y|x')^{-1+\frac{1}{\tau}}\right)^{\alpha-1}\right]^{1/\alpha-1}. &(246)
\end{aligned}$$

$f_{x',Q_Y,x}(\alpha,\tau)$ may be defined by its continuous extension at $\alpha=\infty$, $\tau=\infty$, or $\alpha=1$, (247), as shown at the bottom of the next page.

Looking at (244), for $(\alpha,\tau)\in(1,\infty)\times[1,\infty)$, it is clear that

$$\mathcal{L}_{\alpha,\tau}(X\to Y)=\max_{x'}\inf_{Q_Y}\max_{x}f_{x',Q_Y,x}(\alpha,\tau). \tag{248}$$

We now show that the above equality also holds for $(\alpha,\tau)\in[1,\infty]^2\setminus(1,\infty)\times[1,\infty)$. Employing (247), for $\alpha\in(1,\infty)$ and $\tau=\infty$, we have

$$\begin{aligned}
&\max_{x'}\inf_{Q_Y}\max_{x}f_{x',Q_Y,x}(\alpha,\tau=\infty)\\
&=\mathcal{L}_{\alpha}^{\text{LRDP}}(X\to Y) &(249)\\
&=\mathcal{L}_{\alpha,\tau=\infty}(X\to Y). &(250)
\end{aligned}$$

Similarly, for $\alpha=\tau=\infty$, we have

$$\begin{aligned}
&\max_{x'}\inf_{Q_Y}\max_{x}f_{x',Q_Y,x}(\alpha=\infty,\tau=\infty)\\
&=\mathcal{L}^{\text{LDP}}(X\to Y) &(251)\\
&=\mathcal{L}_{\alpha=\infty,\tau=\infty}(X\to Y). &(252)
\end{aligned}$$

Applying similar steps to equations (211)-(217), for $\alpha=1$ and $\tau\in[1,\infty]$, we have

$$\begin{aligned}
&\max_{x'}\inf_{Q_Y}\max_{x}f_{x',Q_Y,x}(\alpha=1,\tau)\\
&=\mathcal{L}_{\alpha=1,\tau}(X\to Y) &(253)\\
&=\tau\text{-Shannon leakage}. &(254)
\end{aligned}$$

For $\alpha=\infty$ and $\tau\in[1,\infty)$, we have

$$\begin{aligned}
&\max_{x'}\inf_{Q_Y}\max_{x}f_{x',Q_Y,x}(\alpha=\infty,\tau)\\
&=\max_{x'}\inf_{Q_Y}\max_{x,y}\log P_{Y|X}(y|x)\,Q_Y(y)^{-\frac{1}{\tau}}P_{Y|X}(y|x')^{-1+\frac{1}{\tau}} &(255)\\
&=\frac{1}{\tau}\max_{x'}\inf_{Q_Y}\max_{y}\log Q_Y(y)^{-1}\;P_{Y|X}(y|x')^{1-\tau}\\
&\quad\times\max_{x}P_{Y|X}(y|x)^{\tau} &(256)\\
&=\frac{1}{\tau}\max_{x'}\inf_{Q_Y}\max_{y}\log Q_Y(y)^{-1}\\
&\quad\times\frac{P_{Y|X}(y|x')^{1-\tau}\;\max_{x}P_{Y|X}(y|x)^{\tau}}{\sum_{y'}P_{Y|X}(y'|x')^{1-\tau}\;\max_{x}P_{Y|X}(y'|x)^{\tau}}\\
&\quad\times\sum_{y'}P_{Y|X}(y'|x')^{1-\tau}\;\max_{x}P_{Y|X}(y'|x)^{\tau} &(257)\\
&=\frac{1}{\tau}\max_{x'}\left[\log\sum_{y'}P_{Y|X}(y'|x')^{1-\tau}\;\max_{x}P_{Y|X}(y'|x)^{\tau}\right.\\
&\quad+\inf_{Q_Y}\log\max_{y}Q_Y(y)^{-1}\\
&\quad\left.\times\frac{P_{Y|X}(y|x')^{1-\tau}\;\max_{x}P_{Y|X}(y|x)^{\tau}}{\sum_{y'}P_{Y|X}(y'|x')^{1-\tau}\;\max_{x}P_{Y|X}(y'|x)^{\tau}}\right]. &(258)
\end{aligned}$$

Now we show that

$$\inf_{Q_Y}\log\max_{y}Q_Y(y)^{-1}$$

$$Q_{x',P_{\tilde{X}}}(\alpha,\tau)=\begin{cases}\frac{1}{\tau}I(\tilde{X};Y)+\left(1-\frac{1}{\tau}\right)D_{KL}\left(P_{Y|X}(y|x)\|P_{Y|X}(y|x')|P_{\tilde{X}}(x)\right) & \text{if } \alpha=1,\tau\in[1,\infty]\\ \frac{1}{\tau}\log\sum_{y}P_{Y|X}(y|x')^{1-\tau}\max_{x}P_{Y|X}(y|x)^{\tau} & \text{if } \alpha=\infty,\tau\in[1,\infty)\\ \frac{1}{\alpha-1}\log\sum_{x,y}P_{\tilde{X}}(x)P_{Y|X}(y|x')^{1-\alpha}P_{Y|X}(y|x)^{\alpha} & \text{if } \alpha\in(1,\infty),\tau=\infty\\ \max_{x,y}P_{Y|X}(y|x)P_{Y|X}(y|x')^{-1} & \text{if } \alpha=\infty,\tau=\infty.\end{cases} \tag{227}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$\times \frac{P_{Y|X}(y|x')^{1-\tau} \max_x P_{Y|X}(y|x)^{\tau}}{\sum_{y'} P_{Y|X}(y'|x')^{1-\tau} \max_x P_{Y|X}(y'|x)^{\tau}} = 0. \tag{259}$$

Let $g_Y(y) = \frac{P_{Y|X}(y|x')^{1-\tau} \max_x P_{Y|X}(y|x)^{\tau}}{\sum_{y'} P_{Y|X}(y'|x')^{1-\tau} \max_x P_{Y|X}(y'|x)^{\tau}}$ be a distribution on Y. If $Q_Y(y) = g_Y(y)$ for all $y \in \mathcal{Y}$, we have $\log \max_y Q_Y(y)^{-1} g_Y(y) = 0$. So,

$$\inf_{Q_Y} \log \max_y Q_Y(y)^{-1} g_Y(y) \leq 0. \tag{260}$$

Moreover, we have

$$\begin{aligned}
&\inf_{Q_Y} \log \max_y \frac{g_Y(y)}{Q_Y(y)} \\
&= \inf_{Q_Y} \max_y \log \frac{g_Y(y)}{Q_Y(y)} && (261)\\
&= \inf_{Q_Y} \sum_{y'} g_Y(y') \left(\max_y \log \frac{g_Y(y)}{Q_Y(y)} \right) && (262)\\
&\geq \inf_{Q_Y} \sum_{y'} g_Y(y') \log \frac{g_Y(y')}{Q_Y(y')} && (263)\\
&= \inf_{Q_Y} D_{KL}\left(g_Y \| Q_Y\right) = 0. && (264)
\end{aligned}$$

Combining (260) and (264), we get $\inf_{Q_Y} \log \max_y \frac{g_Y(y)}{Q_Y(y)} = 0$. Therefore, (258) collapses to

$$\begin{aligned}
&\frac{1}{\tau} \max_{x'} \log \sum_{y'} P_{Y|X}(y'|x')^{1-\tau} \max_x P_{Y|X}(y'|x)^{\tau} \\
&= \mathcal{L}_{\alpha=\infty,\tau}(X \to Y). && (265)
\end{aligned}$$

This completes the proof of the validity of (248) for all $(\alpha, \tau) \in [1, \infty]^2$.

We now investigate the monotonicity of $f_{x',Q_Y,x}(\alpha, \tau)$ in α and τ. $f_{x',Q_Y,x}(\alpha, \tau)$ is non-decreasing in α for a fixed τ because the quantity inside the logarithm in (246) represents $(\alpha - 1)$-norm of a random variable, and $(\alpha - 1)$-norm of a random variable is non-decreasing in α. In the proof of Lemma 1, we show that $Q_{x',P_{\tilde{X}}}(\alpha, \tau)$ defined in (226) is non-decreasing in τ and so $\sup_{P_{\tilde{X}}} Q_{x',P_{\tilde{X}}}(\alpha, \tau)$ is non-decreasing in τ. Moreover, equations (242)-(244) show that $\inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha, \tau) = \sup_{P_{\tilde{X}}} Q_{x',P_{\tilde{X}}}(\alpha, \tau)$ (note that the infimum of the objective in (242) over Q_Y is equal to $Q_{x',P_{\tilde{X}}}(\alpha, \tau)$). So, $\inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha, \tau)$ is non-decreasing in τ.

For $(\alpha_0, \tau_0) \in [1, \infty]^2$, we have

$$\begin{aligned}
&\lim_{\epsilon \to 0} \sup_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) && (266)\\
&= \lim_{\epsilon \to 0} \mathcal{L}_{\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)}(X \to Y) && (267)\\
&= \lim_{\epsilon \to 0} \max_{x'} \inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (268)\\
&= \max_{x'} \lim_{\epsilon \to 0} \inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (269)\\
&= \max_{x'} \inf_{\epsilon > 0} \inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (270)\\
&= \max_{x'} \inf_{Q_Y} \inf_{\epsilon > 0} \max_x f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (271)\\
&\leq \max_{x'} \inf_{Q_Y} \lim_{\epsilon \to 0} \max_x f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (272)\\
&= \max_{x'} \inf_{Q_Y} \max_x \lim_{\epsilon \to 0} f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0)) && (273)\\
&= \max_{x'} \inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha_0^+(\alpha_0), \tau_0^+(\tau_0)) && (274)\\
&= \max_{x'} \inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha_0, \tau_0) && (275)\\
&= \mathcal{L}_{\alpha_0,\tau_0}(X \to Y), && (276)
\end{aligned}$$

where

- (267) follows because $\mathcal{L}_{\alpha,\tau}(X \to Y)$ is non-decreasing in α and τ.
- (270) follows because $f_{x',Q_Y,x}(\alpha, \tau)$ is non-decreasing in α for a fixed τ and $\inf_{Q_Y} \max_x f_{x',Q_Y,x}(\alpha, \tau)$ is non-decreasing in τ for a fixed α. Moreover, $\alpha_\epsilon^+(\alpha_0)$ and $\tau_\epsilon^+(\tau_0)$ are non-decreasing in ϵ for a fixed α_0 and τ_0, respectively.
- (274) follows because $f_{x',Q_Y,x}(\alpha_\epsilon^+(\alpha_0), \tau_\epsilon^+(\tau_0))$ is continuous in ϵ.

For $(\alpha_0, \tau_0) \in [1, \infty]^2$, combining (241) and (276), we have

$$\begin{aligned}
\mathcal{L}_{\alpha_0,\tau_0}(X \to Y) &= \lim_{\epsilon \to 0} \inf_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \\
&\leq \lim_{\epsilon \to 0} \sup_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \\
&\leq \mathcal{L}_{\alpha_0,\tau_0}(X \to Y). && (277)
\end{aligned}$$

which implies

$$\begin{aligned}
&\lim_{\epsilon \to 0} \inf_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) \\
&= \lim_{\epsilon \to 0} \sup_{\substack{\alpha \in [\alpha_\epsilon^-(\alpha_0), \alpha_\epsilon^+(\alpha_0)], \\ \tau \in [\tau_\epsilon^-(\tau_0), \tau_\epsilon^+(\tau_0)]}} \mathcal{L}_{\alpha,\tau}(X \to Y) && (278)\\
&= \mathcal{L}_{\alpha_0,\tau_0}(X \to Y). && (279)
\end{aligned}$$

$$f_{x',Q_Y,x}(\alpha, \tau) = \begin{cases}
\sum_y P_{Y|X}(y|x) \log \frac{P_{Y|X}(y|x)}{Q_Y(y)^{\frac{1}{\tau}} P_{Y|X}(y|x')^{1-\frac{1}{\tau}}} & \text{if } \alpha = 1, \tau \in [1, \infty] \\
\max_y \log P_{Y|X}(y|x)\, Q_Y(y)^{-\frac{1}{\tau}} P_{Y|X}(y|x')^{-1+\frac{1}{\tau}} & \text{if } \alpha = \infty, \tau \in [1, \infty) \\
D_\alpha\left(P_{Y|X}(y|x) \| P_{Y|X}(y|x')\right) & \text{if } \alpha \in (1, \infty), \tau = \infty \\
\max_y P_{Y|X}(y|x) P_{Y|X}(y|x')^{-1} & \text{if } \alpha = \infty, \tau = \infty.
\end{cases} \tag{247}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

This completes the proof of the continuity of maximal (α,τ)-leakage.

B. Continuity of $\mathcal{L}_{\alpha,\beta}(X\to Y)$ at $(\alpha,\beta)\in[1,\infty]^2\setminus\{(1,1)\}$

Let

$$B_{XY}(\alpha,\beta)=\mathcal{L}_{\alpha,\beta}(X\to Y)$$

and

$$T_{XY}(\alpha,\tau)=\mathcal{L}_{\alpha,\tau}(X\to Y).$$

For $\alpha>\beta$, we have

$$T_{XY}(\alpha,\tau)=B_{XY}\left(\alpha,\frac{\alpha\tau}{\tau+\alpha-1}\right) \tag{280}$$

and

$$B_{XY}(\alpha,\beta)=T_{XY}\left(\alpha,\frac{\beta(\alpha-1)}{\alpha-\beta}\right). \tag{281}$$

To demonstrate the continuity of MαbeL, we employ the sequential continuity theorem, that is, a function f is continuous at a if and only if $f(x_n)\to f(a)$ for all sequences $x_n\to a$.

Continuity at (α_0,β_0) with $\alpha_0>\beta_0$: If $\lim_{n\to\infty}(\alpha_n,\beta_n)=(\alpha_0,\beta_0)$, then for sufficiently large n, we have $\alpha_n>\beta_n$ and so

$$\begin{aligned}
&\lim_{n\to\infty}B_{XY}(\alpha_n,\beta_n)\\
&=\lim_{n\to\infty}T_{XY}\left(\alpha_n,\frac{\beta_n(\alpha_n-1)}{\alpha_n-\beta_n}\right) &(282)\\
&=T_{XY}\left(\lim_{n\to\infty}\alpha_n,\lim_{n\to\infty}\frac{\beta_n(\alpha_n-1)}{\alpha_n-\beta_n}\right) &(283)\\
&=T_{XY}\left(\alpha_0,\frac{\beta_0(\alpha_0-1)}{\alpha_0-\beta_0}\right) &(284)\\
&=B_{XY}(\alpha_0,\beta_0), &(285)
\end{aligned}$$

where (283) and (284) follow from the continuity of maximal (α,τ)-leakage and the continuity of $\frac{\beta(\alpha-1)}{\alpha-\beta}$ for $\alpha>\beta$, respectively.

Continuity at (α_0,β_0) with $1\neq\alpha_0<\beta_0$: We first prove the continuity of $\mathcal{L}_\beta^{\text{LRDP}}(X\to Y)$ at $\beta>1$ as follows. If $\lim_{n\to\infty}\beta_n=\beta\neq1$, then we have

$$\begin{aligned}
&\lim_{n\to\infty}\mathcal{L}_{\beta_n}^{\text{LRDP}}(X\to Y)\\
&=\lim_{n\to\infty}\max_{x,x'\in\mathcal{X}}\frac{1}{\beta_n-1}\log\sum_y P_{Y|X}(y|x')^{1-\beta_n}\\
&\quad\times P_{Y|X}(y|x)^{\beta_n} &(286)\\
&=\max_{x,x'\in\mathcal{X}}\lim_{n\to\infty}\frac{1}{\beta_n-1}\log\sum_y P_{Y|X}(y|x')^{1-\beta_n}\\
&\quad\times P_{Y|X}(y|x)^{\beta_n} &(287)\\
&=\max_{x,x'\in\mathcal{X}}\frac{1}{\beta-1}\log\sum_y P_{Y|X}(y|x')^{1-\beta}P_{Y|X}(y|x)^{\beta} &(288)\\
&=\mathcal{L}_\beta^{\text{LRDP}}(X\to Y), &(289)
\end{aligned}$$

where (288) follows because the objective is continuous at $\beta>1$. Note that the objective is defined by its continuous extension, i.e., KL divergence, at $\beta=1$. If $\lim_{n\to\infty}(\alpha_n,\beta_n)=(\alpha_0,\beta_0)$ with $1\neq\alpha_0<\beta_0$, then for sufficiently large n, we have $1\neq\alpha_n<\beta_n$. So,

$$\begin{aligned}
&\lim_{n\to\infty}\mathcal{L}_{\alpha_n,\beta_n}(X\to Y)\\
&=\lim_{n\to\infty}\frac{\alpha_n(\beta_n-1)}{(\alpha_n-1)\beta_n}\,\mathcal{L}_{\beta_n}^{\text{LRDP}}(X\to Y) &(290)\\
&=\frac{\alpha_0(\beta_0-1)}{(\alpha_0-1)\beta_0}\,\mathcal{L}_{\beta_0}^{\text{LRDP}}(X\to Y) &(291)\\
&=\mathcal{L}_{\alpha_0,\beta_0}(X\to Y), &(292)
\end{aligned}$$

where (291) follows from the continuity of $\mathcal{L}_\beta^{\text{LRDP}}(X\to Y)$ and $\frac{\alpha(\beta-1)}{(\alpha-1)\beta}$ for $\alpha\neq1$.

Continuity at (α_0,β_0) with $1=\alpha_0<\beta_0$:

Let $\lim_{n\to\infty}(\alpha_n,\beta_n)=(1,\beta_0\neq1)$. If $\mathcal{L}_{\beta_0}^{\text{LRDP}}(X\to Y)\neq0$, for sufficiently large n, we have

$$\begin{aligned}
&\lim_{n\to\infty}\mathcal{L}_{\alpha_n,\beta_n}(X\to Y)\\
&=\lim_{n\to\infty}\frac{\alpha_n(\beta_n-1)}{(\alpha_n-1)\beta_n}\,\mathcal{L}_{\beta_n}^{\text{LRDP}}(X\to Y) &(293)\\
&=\infty. &(294)
\end{aligned}$$

Here, maximal (α,β)-leakage is continuous in the sense that the limit points of all the sequences $\{\mathcal{L}_{\alpha_n,\beta_n}(X\to Y)\}_{n\in\mathbb{N}}$ are equal to ∞. Moreover, if $\mathcal{L}_{\beta_0}^{\text{LRDP}}(X\to Y)=0$, then X and Y are independent. So, $\mathcal{L}_{\alpha,\beta}(X\to Y)=0$ everywhere and is continuous.

Continuity at (α_0,β_0) with $\alpha_0=\beta_0\neq1$: Let

$$\lim_{n\to\infty}(\alpha_n,\beta_n)=(\beta_0,\beta_0)\neq(1,1),$$

and let partition $\{(\alpha_n,\beta_n)\}_{n\in\mathbb{N}}$ into two distinct subsequences $\{(\alpha_{n_k},\beta_{n_k})\}_{k\in S_1}$ with $\alpha_{n_k}\le\beta_{n_k}$ and $\{(\alpha_{\bar n_k},\beta_{\bar n_k})\}_{k\in S_2}$ with $\alpha_{\bar n_k}>\beta_{\bar n_k}$, where $\{n_k\}_{k\in S_1}\cup\{\bar n_k\}_{k\in S_2}=\mathbb{N}$ and $S_1,S_2\subseteq\mathbb{N}$. If either of the subsequences is finite, then the sequence $\{(\alpha_n,\beta_n)\}_{n>N}$ with $N>\min\{\max_{k\in S_1}n_k,\max_{k\in S_2}\bar n_k\}$ consists entirely of elements from the other subsequence. As a result, this finite subsequence does not impact the convergence of the original sequence $\{(\alpha_n,\beta_n)\}_{n\in\mathbb{N}}$. Here, we consider the scenario where $S_1=S_2=\mathbb{N}$. Since every subsequence of a convergent sequence converges to the same limit as the original sequence, we have $\lim_{k\to\infty}(\alpha_{n_k},\beta_{n_k})=(\beta_0,\beta_0)$ and $\lim_{k\to\infty}(\alpha_{\bar n_k},\beta_{\bar n_k})=(\beta_0,\beta_0)$. For $\{(\alpha_{n_k},\beta_{n_k})\}_{k\in\mathbb{N}}$ with $\alpha_{n_k}\le\beta_{n_k}$, we have

$$\begin{aligned}
&\lim_{k\to\infty}\mathcal{L}_{\alpha_{n_k},\beta_{n_k}}(X\to Y)\\
&=\lim_{k\to\infty}\frac{\alpha_{n_k}(\beta_{n_k}-1)}{(\alpha_{n_k}-1)\beta_{n_k}}\,\mathcal{L}_{\beta_{n_k}}^{\text{LRDP}}(X\to Y) &(295)\\
&=\mathcal{L}_{\beta_0}^{\text{LRDP}}(X\to Y). &(296)
\end{aligned}$$

The last equality follows from the continuity of $\mathcal{L}_\beta^{\text{LRDP}}(X\to Y)$ and $\frac{\alpha(\beta-1)}{(\alpha-1)\beta}$ for $\alpha\neq1$. Furthermore, recalling the functions $B_{XY}(\alpha,\beta)$ and $T_{XY}(\alpha,\tau)$, for $\{(\alpha_{\bar n_k},\beta_{\bar n_k})\}_{k\in\mathbb{N}}$ with $\alpha_{\bar n_k}>\beta_{\bar n_k}$, we have

$$\lim_{k\to\infty}\mathcal{L}_{\alpha_{\bar n_k},\beta_{\bar n_k}}(X\to Y)$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \lim_{k\to\infty} B_{XY}(\alpha_{\bar{n}_k}, \beta_{\bar{n}_k}) \tag{297}$$

$$= \lim_{k\to\infty} T_{XY}\left(\alpha_{\bar{n}_k}, \frac{\beta_{\bar{n}_k}(\alpha_{\bar{n}_k}-1)}{\alpha_{\bar{n}_k}-\beta_{\bar{n}_k}}\right) \tag{298}$$

$$= T_{XY}\left(\lim_{k\to\infty} \alpha_{\bar{n}_k}, \lim_{k\to\infty} \frac{\beta_{\bar{n}_k}(\alpha_{\bar{n}_k}-1)}{\alpha_{\bar{n}_k}-\beta_{\bar{n}_k}}\right) \tag{299}$$

$$= T_{XY}(\beta_0, \infty) \tag{300}$$

$$= \mathcal{L}^{\text{LRDP}}_{\beta_0}(X \to Y) \tag{301}$$

where (299) follows from the continuity of $\mathcal{L}_{\alpha,\tau}(X \to Y)$ and (301) follows because

$$\lim_{\tau\to\infty} \mathcal{L}_{\alpha,\tau}(X \to Y) = \mathcal{L}^{\text{LRDP}}_{\alpha}(X \to Y).$$

Combining (296) and (301), we get

$$\lim_{n\to\infty} \mathcal{L}_{\alpha_n,\beta_n}(X \to Y) = \mathcal{L}^{\text{LRDP}}_{\beta_0}(X \to Y).$$

This completes the proof of continuity.

Appendix K
Proof of Theorem 7

Here, we extend our results to continuous real random variables through the Riemann integral. The results can also be extended to higher dimensions through Lebesgue integral. We first consider a case in which X still has a finite alphabet $\mathcal{X}$ but Y takes value from a continuous alphabet $\mathcal{Y} \subseteq \mathbb{R}$.

Lemma 2: When X has a finite alphabet and Y is continuous, maximal (α, β)-leakage defined in (13) simplifies to

$$\mathcal{L}_{\alpha,\beta}(X \to Y) = \sup_{P_X} \sup_{P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha}\right)^{\frac{\beta}{\alpha}} dy \tag{302}$$

where $P_{\tilde{X}}$ is a distribution on the support of P_X.

The proof of lemma 2 follows similar steps to the proof of Theorem 1 along the lines of [16, Proof of Theorem 7]. Using lemma 2, we prove Theorem 7 as follows.

Upper Bound: Applying similar steps to the proof of upper bound for Theorem 1, we may get

$$\mathcal{L}_{\alpha,\beta}(X \to Y) \le \sup_{f_X} \sup_{f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} dx\right)^{\frac{\beta}{\alpha}} dy. \tag{303}$$

Lower Bound: Fix $n_1, n_2 \in \mathbb{N}$ and $a, b \in \mathbb{R}$ such that $a, b > 0$. We partition the intervals $[-a, a]$ and $[-b, b]$ into subintervals with equal lengths $\Delta_1 = \frac{2a}{n_1}$ and $\Delta_2 = \frac{2b}{n_2}$, respectively. Let

$$\bar{X} = \sum_{i=1}^{n_1} x_i^* \ \mathbb{1}\{X \in [-a + (i-1)\Delta_1, -a + i\Delta_1]\}$$

for $x \in [-a, a]$, and $\bar{X} = x_0^*$, otherwise. Moreover, let

$$\bar{Y} = \sum_{j=1}^{n_2} y_j^* \ \mathbb{1}\{Y \in [-b + (j-1)\Delta_2, -b + j\Delta_2]\}$$

for $y \in [-b, b]$, and $\bar{Y} = y_0^*$, otherwise. Here, $\mathbb{1}\{\cdot\}$ is the indicator function. Furthermore, $x_i^* \in [-a + (i-1)\Delta_1, -a + i\Delta_1]$ for $i \in \{1, \cdots, n_1\}$ and $y_j^* \in [-b + (j-1)\Delta_2, -b + j\Delta_2]$ for $j \in \{1, \cdots, n_2\}$ are fixed points, and x_0^* and y_0^* are fixed symbols. For continuous random variables X and Y and their quantized versions $\bar{X}$ and $\bar{Y}$, we now prove that since the Markov chain $\bar{X} - X - Y - \bar{Y}$ holds, we have $\mathcal{L}_{\alpha,\beta}(X \to Y) \ge \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$. To do so, we first prove $\mathcal{L}_{\alpha,\beta}(X \to Y) \ge \mathcal{L}_{\alpha,\beta}(\bar{X} \to Y)$ and then, we show $\mathcal{L}_{\alpha,\beta}(\bar{X} \to Y) \ge \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$. At the end, we bound $\mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$ from below. Applying similar steps to the proof of the linkage inequality for random variables with finite alphabets, i.e., (16b), we may prove the following lemma.

Lemma 3: Let X have a finite alphabet and Y and Z be continuous random variables. If the Markov chain $X - Y - Z$ holds then $\mathcal{L}_{\alpha,\beta}(Y \to Z) \ge \mathcal{L}_{\alpha,\beta}(X \to Z)$, which means

$$\mathcal{L}_{\alpha,\beta}(X \to Y) \ge \mathcal{L}_{\alpha,\beta}(\bar{X} \to Y). \tag{304}$$

Using lemma 2, we prove the following post-processing inequality.

Lemma 4: Let X and Z have finite alphabets and Y be a continuous random variable. If the Markov chain $X - Y - Z$ holds then $\mathcal{L}_{\alpha,\beta}(X \to Y) \ge \mathcal{L}_{\alpha,\beta}(X \to Z)$.

Proof: For any $y \in \mathcal{Y}$, let

$$g(y) = \left(\sum_x P_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha}\right)^{\frac{1}{\alpha}} \tag{305}$$

and

$$c_z(y) = \frac{f_Y(y)\ P_{Z|Y}(z|y)}{P_Z(z)} \tag{306}$$

such that $\int_{\mathcal{Y}} c_z(y)\ dy = 1$. We have

$$\int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha}\right)^{\frac{\beta}{\alpha}} dy \tag{307}$$

$$= \int_{\mathcal{Y}} f_Y(y)^{1-\beta} g(y)^{\beta} dy \tag{308}$$

$$= \int_{\mathcal{Y}} \sum_z f_Y(y) P_{Z|Y}(z|y) \left(\frac{g(y)}{f_Y(y)}\right)^{\beta} dy \tag{309}$$

$$= \sum_z P_Z(z) \int_{\mathcal{Y}} c_z(y) \left(\frac{g(y)}{f_Y(y)}\right)^{\beta} dy \tag{310}$$

$$\ge \sum_z P_Z(z) \left(\int_{\mathcal{Y}} c_z(y) \frac{g(y)}{f_Y(y)}\ dy\right)^{\beta} \tag{311}$$

$$= \sum_z P_Z(z)^{1-\beta} \left(\int_{\mathcal{Y}} P_{Z|Y}(z|y) g(y)\ dy\right)^{\beta} \tag{312}$$

where (311) follows from applying Jensen's inequality to the convex function $f:\ x \to x^p$ $(x \ge 0,\ p \ge 1)$. Recalling the definition of $g(y)$ from (305), we have

$$\int_{\mathcal{Y}} P_{Z|Y}(z|y) g(y)\ dy \tag{313}$$

$$= \int_{\mathcal{Y}} P_{Z|Y}(z|y) \left(\sum_x P_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha}\right)^{\frac{1}{\alpha}} dy \tag{314}$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \int_{\mathcal{Y}} \left(\sum_x \left(P_{\tilde{X}}(x)^{\frac{1}{\alpha}} P_{Z|Y}(z|y) f_{Y|X}(y|x) \right)^{\alpha} \right)^{\frac{1}{\alpha}} dy \quad (315)$$

$$\geq \left(\sum_x \left(\int_{\mathcal{Y}} P_{\tilde{X}}(x)^{\frac{1}{\alpha}} P_{Z|Y}(z|y) f_{Y|X}(y|x)\ dy \right)^{\alpha} \right)^{\frac{1}{\alpha}} \quad (316)$$

$$= \left(\sum_x P_{\tilde{X}}(x) P_{Z|X}(z|x)^{\alpha} \right)^{\frac{1}{\alpha}} \quad (317)$$

where

- (316) follows from Minkowski's integral inequality,
- (317) follows because the Markov chain $X-Y-Z$ holds.

Applying (317) to (312), and using the fact that for $\alpha \in (1,\infty)$ and $\beta \in [1,\infty)$, the function $f : t \to \frac{\alpha}{(\alpha-1)\beta} \log t$ is increasing in $t > 0$, give

$$\frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} \right)^{\frac{\beta}{\alpha}} dy$$
$$\geq \frac{\alpha}{(\alpha-1)\beta} \log \sum_z P_Z(z)^{1-\beta} \left(\sum_x P_{\tilde{X}}(x) P_{Z|X}(z|x)^{\alpha} \right)^{\frac{\beta}{\alpha}}. \quad (318)$$

Taking suprema over P_X and $P_{\tilde{X}}$ completes the proof. □

From lemma 4, we get $\mathcal{L}_{\alpha,\beta}(\bar{X} \to Y) \geq \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$. Combining this result with (304), we have $\mathcal{L}_{\alpha,\beta}(X \to Y) \geq \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$. Since $\mathcal{L}_{\alpha,\beta}(X \to Y) \geq \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$ holds for all $a, b > 0$ and $n_1, n_2 \in \mathbb{N}$, we get $\mathcal{L}_{\alpha,\beta}(X \to Y) \geq \sup_{a,b,n_1,n_2} \mathcal{L}_{\alpha,\beta}(\bar{X} \to \bar{Y})$. Moreover, since $\bar{X}$ and $\bar{Y}$ have finite alphabets, we may use the result of lower bound for Theorem 1, equation (65), and so we have

$$\mathcal{L}_{\alpha,\beta}(X \to Y)$$
$$\geq \sup_{a,b,n_1,n_2} \sup_{P_{\bar{X}},P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_{j=0}^{n_2} P_{\bar{Y}}(y_j^*)^{1-\beta} \left(\sum_{i=0}^{n_1} P_{\tilde{X}}(x_i^*) P_{\bar{Y}|\bar{X}}(y_j^*|x_i^*)^{\alpha} \right)^{\frac{\beta}{\alpha}} \quad (319)$$

$$\geq \sup_{P_{\bar{X}},P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sup_{a,b,n_1,n_2} \sum_{j=1}^{n_2} P_{\bar{Y}}(y_j^*)^{1-\beta} \left(\sum_{i=1}^{n_1} P_{\tilde{X}}(x_i^*) P_{\bar{Y}|\bar{X}}(y_j^*|x_i^*)^{\alpha} \right)^{\frac{\beta}{\alpha}} \quad (320)$$

$$\geq \sup_{P_{\bar{X}},P_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sup_{b,n_2} \sum_{j=1}^{n_2} P_{\bar{Y}}(y_j^*)^{1-\beta} \left(\lim_{a\to\infty} \lim_{n_1\to\infty} \sum_{i=1}^{n_1} P_{\tilde{X}}(x_i^*) P_{\bar{Y}|\bar{X}}(y_j^*|x_i^*)^{\alpha} \right)^{\frac{\beta}{\alpha}} \quad (321)$$

$$= \sup_{f_{\bar{X}},f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sup_{b,n_2} \sum_{j=1}^{n_2} P_{\bar{Y}}(y_j^*)^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) P_{\bar{Y}|X}(y_j^*|x)^{\alpha} dx \right)^{\frac{\beta}{\alpha}} \quad (322)$$

$$\geq \sup_{f_{\bar{X}},f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \lim_{b\to\infty} \lim_{n_2\to\infty} \sum_{\substack{j=1:\\ P_{\bar{Y}}(y_j^*)>0}}^{n_2} P_{\bar{Y}}(y_j^*) \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) \left(\frac{P_{\bar{Y}|X}(y_j^*|x)}{P_{\bar{Y}}(y_j^*)} \right)^{\alpha} dx \right)^{\frac{\beta}{\alpha}} \quad (323)$$

$$= \sup_{f_{\bar{X}},f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y) \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) \left(\frac{f_{Y|X}(y|x)}{f_Y(y)} \right)^{\alpha} dx \right)^{\frac{\beta}{\alpha}} dy \quad (324)$$

$$= \sup_{f_{\bar{X}},f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} dx \right)^{\frac{\beta}{\alpha}} dy \quad (325)$$

where $P_{\tilde{X}}$ is a distribution on the support of $\bar{X}$, f_X is the marginal pdf of X and $f_{\tilde{X}}$ is a pdf on the support of X. Furthermore, (322) and (324) follow from the definition of the Riemann integral. Combining (303) and (325) gives

$$\mathcal{L}_{\alpha,\beta}(X \to Y)$$
$$= \sup_{f_X} \sup_{f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_Y(y)^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} dx \right)^{\frac{\beta}{\alpha}} dy \quad (326)$$

$$= \max_{x':f_X(x')>0} \sup_{f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \int_{\mathcal{Y}} f_{Y|X}(y|x')^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) f_{Y|X}(y|x)^{\alpha} dx \right)^{\beta/\alpha} dy \quad (327)$$

where the latter equality follows because the quantity inside the log is convex in f_X. Similarly, we may prove the following lemma.

Lemma 5: When X is continuous and Y has a finite alphabet, maximal (α,β)-leakage defined in (13) simplifies to

$$\mathcal{L}_{\alpha,\beta}(X \to Y)$$
$$= \max_{x':f_X(x')>0} \sup_{f_{\tilde{X}}} \frac{\alpha}{(\alpha-1)\beta} \log \sum_y P_{Y|X}(y|x')^{1-\beta} \left(\int_{\mathcal{X}} f_{\tilde{X}}(x) P_{Y|X}(y|x)^{\alpha} dx \right)^{\beta/\alpha} \quad (328)$$

where $f_{\tilde{X}}$ is a pdf on $\mathcal{X}$.

Appendix L
Results for Known Mechanisms VI-A

Here, we obtain an upper bound on vector maximal Renyi leakage under a Laplacian mechanism. The proof for a Gaussian mechanism follows similarly.

Let $c_{i,x_{-i}} = \max_{x_i} h(x_{-i}, x_i)$, $a_{i,x_{-i}} = \min_{x_i} h(x_{-i}, x_i)$, and $Y = \mathcal{M}(X^n)$. Since $|h(x_{-i}, x_i) - h(x_{-i}, \tilde{x}_i)| \leq \delta$, we have $c_{i,x_{-i}} - a_{i,x_{-i}} \leq \delta$. Moreover, for continuous alphabets we have

$$\max_i \mathcal{L}_{\infty,\beta}(X_i \to Y|X_{-i})$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$= \max_i \max_{\tilde{x}_i, x_{-i}} \frac{1}{\beta} \log \int_{-\infty}^{\infty} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} f_{Y|X_i,X_{-i}}(y|x_i, x_{-i})^{\beta} \, dy, \tag{329}$$

where

$$f_{Y|X_i,X_{-i}}(y|x_i, x_{-i}) = f_N\left(y - h(x_{-i}, x_i)\right)$$

and

$$f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i}) = f_N\left(y - h(x_{-i}, \tilde{x}_i)\right).$$

For fixed $i, \tilde{x}_i$ and x_{-i}, consider the quantity inside the logarithm:

$$\int_{-\infty}^{\infty} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} f_{Y|X_i,X_{-i}}(y|x_i, x_{-i})^{\beta} \, dy \tag{330}$$

$$= (\frac{1}{2b})^{\beta} \int_{-\infty}^{\infty} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} \exp - \frac{\beta|y - h(x_{-i}, x_i)|}{b} \, dy \tag{331}$$

$$= (\frac{1}{2b})^{\beta} \Bigg[\int_{-\infty}^{a_{i,x_{-i}}} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} \exp - \frac{\beta|y - h(x_{-i}, x_i)|}{b} \, dy + \int_{a_{i,x_{-i}}}^{c_{i,x_{-i}}} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} \exp - \frac{\beta|y - h(x_{-i}, x_i)|}{b} \, dy + \int_{c_{i,x_{-i}}}^{\infty} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \max_{x_i} \exp - \frac{\beta|y - h(x_{-i}, x_i)|}{b} \, dy \Bigg] \tag{332}$$

$$\leq (\frac{1}{2b})^{\beta} \Bigg[\int_{-\infty}^{a_{i,x_{-i}}} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \times \exp - \frac{\beta|y - a_{i,x_{-i}}|}{b} \, dy + \int_{a_{i,x_{-i}}}^{c_{i,x_{-i}}} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \, dy + \int_{c_{i,x_{-i}}}^{\infty} f_{Y|X_i,X_{-i}}(y|\tilde{x}_i, x_{-i})^{1-\beta} \exp - \frac{\beta|y - c_{i,x_{-i}}|}{b} \, dy \Bigg] \tag{333}$$

$$= \frac{1}{2b} \Bigg[\int_{-\infty}^{a_{i,x_{-i}}} \exp \frac{(\beta-1)|y - h(x_{-i}, \tilde{x}_i)|}{b} \times \exp - \frac{\beta|y - a_{i,x_{-i}}|}{b} \, dy + \int_{a_{i,x_{-i}}}^{c_{i,x_{-i}}} \exp \frac{(\beta-1)|y - h(x_{-i}, \tilde{x}_i)|}{b} \, dy + \int_{c_{i,x_{-i}}}^{\infty} \exp \frac{(\beta-1)|y - h(x_{-i}, \tilde{x}_i)|}{b} \times \exp - \frac{\beta|y - c_{i,x_{-i}}|}{b} \, dy \Bigg] \tag{334}$$

$$= \frac{1}{2b} \Bigg[\int_{-\infty}^{a_{i,x_{-i}}} \exp \frac{(1-\beta)(y - h(x_{-i}, \tilde{x}_i))}{b} \times \exp \frac{\beta(y - a_{i,x_{-i}})}{b} \, dy + \int_{a_{i,x_{-i}}}^{h(x_{-i},\tilde{x}_i)} \exp \frac{(1-\beta)(y - h(x_{-i}, \tilde{x}_i))}{b} \, dy + \int_{h(x_{-i},\tilde{x}_i)}^{c_{i,x_{-i}}} \exp \frac{(\beta-1)(y - h(x_{-i}, \tilde{x}_i))}{b} \, dy + \int_{c_{i,x_{-i}}}^{\infty} \exp \frac{(\beta-1)(y - h(x_{-i}, \tilde{x}_i))}{b} \times \exp - \frac{\beta(y - c_{i,x_{-i}})}{b} \, dy \Bigg] \tag{335}$$

$$= \frac{1}{2} \exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \frac{1}{2} \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) + \frac{1}{2(\beta-1)} \Bigg[\exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) - 2 \Bigg] \tag{336}$$

Thus, we have

$$\max_i \mathcal{L}_{\infty,\beta}(X_i \to Y|X_{-i}) \leq \max_{i,\tilde{x}_i,x_{-i}} \frac{1}{\beta} \log \Bigg[\frac{1}{2} \exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \frac{1}{2} \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) + \frac{1}{2(\beta-1)} \left(\exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) - 2 \right) \Bigg] \tag{337}$$

$$= \max_{i,x_{-i}} \max_{h(x_{-i},\tilde{x}_i) \in [a_{i,x_{-i}}, c_{i,x_{-i}}]} \frac{1}{\beta} \log \Bigg[\frac{1}{2} \exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \frac{1}{2} \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) + \frac{1}{2(\beta-1)} \left(\exp\left(\frac{(\beta-1)(h(x_{-i}, \tilde{x}_i) - a_{i,x_{-i}})}{b}\right) + \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - h(x_{-i}, \tilde{x}_i))}{b}\right) - 2 \right) \Bigg] \tag{338}$$

$$= \max_{i,x_{-i}} \frac{1}{\beta} \log \Bigg[\frac{1}{2} - \frac{1}{2(\beta-1)} + \left(\frac{1}{2} + \frac{1}{2(\beta-1)}\right) \exp\left(\frac{(\beta-1)(c_{i,x_{-i}} - a_{i,x_{-i}})}{b}\right) \Bigg] \tag{339}$$

$$\leq \frac{1}{\beta} \log \Bigg[\frac{1}{2} - \frac{1}{2(\beta-1)} + \left(\frac{1}{2} + \frac{1}{2(\beta-1)}\right)$$

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

$$\exp\left(\frac{(\beta-1)\delta}{b}\right)\Bigg], \tag{340}$$

where (339) follows because the quantity inside the logarithm is convex in $h(x_{-i}, \tilde{x_i})$ and so we have $h(x_{-i}, \tilde{x_i}) = a$ or $h(x_{-i}, \tilde{x_i}) = c$. It is easy to show that both values of $h(x_{-i}, \tilde{x_i})$ give the expression (339). Moreover, (340) follows because $c_{i,x_{-i}} - a_{i,x_{-i}} \leq \delta$. The equality is achieved if there exist i and x_{-i} such that the function $h(x_{-i}, x_i)$ from $\mathcal{X}$ to $[a_{i,x_{-i}}, c_{i,x_{-i}}]$ is surjective and $c_{i,x_{-i}} - a_{i,x_{-i}} = \delta$.

References

[1] A. Gilani, G. R. Kurri, O. Kosut, and L. Sankar, "An alphabet of leakage measures," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Nov. 2022, pp. 458–463.

[2] C. Dwork, "Differential privacy," in *Proc. Automata, Lang. Program.*, 2006, pp. 1–12.

[3] G. Smith, "On the foundations of quantitative information flow," in *Proc. Int. Conf. Found. Softw. Sci. Comput. Struct.*, 2009, pp. 288–302.

[4] C. Braun, K. Chatzikokolakis, and C. Palamidessi, "Quantitative notions of leakage for one-try attacks," *Electron. Notes Theor. Comput. Sci.*, vol. 249, pp. 75–91, Aug. 2009.

[5] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, "What can we learn privately?" *SIAM J. Comput.*, vol. 40, no. 3, pp. 793–826, 2011.

[6] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, "Local privacy and statistical minimax rates," in *Proc. IEEE Symp. Found. Comput. Sci.*, Oct. 2013, pp. 429–438.

[7] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *Proc. IEEE 25th Comput. Secur. Found. Symp.*, Jun. 2012, pp. 265–279.

[8] M. S. Alvim, K. Chatzikokolakis, A. Mciver, C. Morgan, C. Palamidessi, and G. Smith, "Additive and multiplicative notions of leakage, and their capacities," in *Proc. IEEE 27th Comput. Secur. Found. Symp.*, Jul. 2014, pp. 308–322.

[9] N. Merhav and E. Arikan, "The Shannon cipher system with a guessing wiretapper," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1860–1866, May 1999.

[10] F. D. P. Calmon and N. Fawaz, "Privacy against statistical inference," in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1401–1408.

[11] C. Schieler and P. Cuff, "The henchman problem: Measuring secrecy by the minimum distortion in a list," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2014, pp. 596–600.

[12] I. Issa and A. B. Wagner, "Measuring secrecy by the probability of a successful guess," in *Proc. 53rd Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Sep. 2015, pp. 980–987.

[13] S. Asoodeh, F. Alajaji, and T. Linder, "On maximal correlation, mutual information and data privacy," in *Proc. IEEE 14th Can. Workshop Inf. Theory (CWIT)*, Jul. 2015, pp. 27–31.

[14] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, "Privacy-aware guessing efficiency," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 754–758.

[15] I. Mironov, "Renyi differential privacy," in *Proc. IEEE 30th Comput. Secur. Found. Symp. (CSF)*, Aug. 2017, pp. 263–275.

[16] I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," *IEEE Trans. Inf. Theory*, vol. 66, no. 3, pp. 1625–1657, Mar. 2020.

[17] J. Liao, O. Kosut, L. Sankar, and F. D. P. Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8043–8066, Dec. 2019.

[18] B. Rassouli and D. Gündüz, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 594–603, 2020.

[19] S. Saeidian, G. Cervia, T. J. Oechtering, and M. Skoglund, "Quantifying membership privacy via information leakage," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3096–3108, 2021.

[20] S. Saeidian, G. Cervia, T. J. Oechtering, and M. Skoglund, "Pointwise maximal leakage," 2022, *arXiv:2205.04935*.

[21] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," in *Proc. Int. Conf. Mach. Learn.*, 2015, pp. 1376–1385.

[22] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Statist. Probab., Contributions Theory Statist.*, vol. 1, 1961, pp. 547–561.

[23] S. Saeidian, G. Cervia, T. J. Oechtering, and M. Skoglund, "Optimal maximal leakage-distortion tradeoff," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2021, pp. 1–6.

[24] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy: On the trade-off between utility and information leakage," in *Proc. Int. Workshop Formal Aspects Secur. Trust*, 2012, pp. 39–54.

[25] J. Liao, L. Sankar, F. P. Calmon, and V. Y. F. Tan, "Hypothesis testing under maximal leakage privacy constraints," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 779–783.

[26] Y. Liu, L. Ong, S. Johnson, J. Kliewer, P. Sadeghi, and P. L. Yeoh, "Information leakage in zero-error source coding: A graph-theoretic perspective," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 2590–2595.

[27] J. M. Abowd, "The US census bureau adopts differential privacy," in *Proc. 24th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2018, p. 2867.

[28] R. Aljably, Y. Tian, M. Al-Rodhaan, and A. Al-Dhelaan, "Anomaly detection over differential preserved privacy in online social networks," *PLoS ONE*, vol. 14, no. 4, Apr. 2019, Art. no. e0215856.

[29] N. Sathyavageeswaran, R. D. Yates, A. D. Sarwate, and N. Mandayam, "Privacy leakage in discrete-time updating systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 2076–2081.

[30] M. Abadi et al., "Deep learning with differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 308–318.

[31] J. Geumlek, S. Song, and K. Chaudhuri, "Renyi differential privacy mechanisms for posterior sampling," in *Proc. Adv. Neural Inf. Process. Syst.*, vol. 30, 2017, pp. 1–10.

[32] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2007, pp. 94–103.

[33] Y. O. Basciftci, Y. Wang, and P. Ishwar, "On privacy-utility tradeoffs for constrained data release mechanisms," in *Proc. Inf. Theory Appl. Workshop (ITA)*, Jan. 2016, pp. 1–6.

[34] G. R. Kurri, L. Sankar, and O. Kosut, "An operational approach to information leakage via generalized gain functions," 2022, *arXiv:2209.13862*.

[35] F. P. Calmon, M. Varia, M. Médard, M. M. Christiansen, K. R. Duffy, and S. Tessaro, "Bounds on inference," in *Proc. 51st Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2013, pp. 567–574.

[36] C. T. Li and A. El Gamal, "Maximal correlation secrecy," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3916–3926, May 2018.

[37] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[38] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. IEEE Inf. Theory Workshop*, Sep. 2007, pp. 442–447.

[39] H. Tyagi, P. Narayan, and P. Gupta, "When is a function securely computable?" *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6337–6350, Oct. 2011.

[40] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[41] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 9, pp. 5018–5029, Sep. 2016.

[42] S. Kamel, M. Sarkiss, M. Wigger, and G. R.-B. Othman, "Secrecy capacity-memory tradeoff of erasure broadcast channels," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5094–5124, Aug. 2019.

[43] F. McSherry, "Privacy integrated queries: An extensible platform for privacy-preserving data analysis," *Commun. ACM*, vol. 53, no. 9, pp. 89–97, 2010.

[44] J. Soria-Comas and J. Domingo-Ferrert, "Differential privacy via t-closeness in data publishing," in *Proc. 11th Annu. Conf. Privacy, Secur. Trust*, Jul. 2013, pp. 27–35.

[45] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, 2006, pp. 486–503.

[46] A. Bittau et al., "Prochlo: Strong privacy for analytics in the crowd," in *Proc. 26th Symp. Operating Syst. Princ.*, Oct. 2017, pp. 441–459.

[47] A. Cheu, A. Smith, J. Ullman, D. Zeber, and M. Zhilyaev, "Distributed differential privacy via shuffling," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Germany: Springer, 2019, pp. 375–403.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.

[48] V. Feldman, A. McMillan, and K. Talwar, "Hiding among the clones: A simple and nearly optimal analysis of privacy amplification by shuffling," in *Proc. Annu. Symp. Found. Comput. Sci. (FOCS)*, 2022, pp. 954–964.

[49] A. M. Girgis, D. Data, S. Diggavi, A. T. Suresh, and P. Kairouz, "On the Renyi differential privacy of the shuffle model," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2021, pp. 2321–2341.

[50] M. Joseph, J. Mao, S. Neel, and A. Roth, "The role of interactivity in local differential privacy," in *Proc. Annu. Symp. Found. Comput. Sci. (FOCS)*, 2019, pp. 94–105.

[51] I. Wagner and D. Eckhoff, "Technical privacy metrics: A systematic survey," *ACM Comput. Surv.*, vol. 51, no. 3, pp. 1–38, Jun. 2018.

[52] M. Bloch et al., "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, Mar. 2021.

[53] H. Hsu, N. Martinez, M. Bertran, G. Sapiro, and F. P. Calmon, "A survey on statistical, information, and estimation—Theoretic views on privacy," *IEEE BITS Inf. Theory Mag.*, vol. 1, no. 1, pp. 45–56, Sep. 2021.

[54] R. Sibson, "Information radius," *Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete*, vol. 14, no. 2, pp. 149–160, 1969.

[55] J. Liao, L. Sankar, O. Kosut, and F. P. Calmon, "Robustness of maximal α-leakage to side information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2019, pp. 642–646.

[56] A. R. Esposito, D. Wu, and M. Gastpar, "On conditional sibson's α-mutual information," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2021, pp. 1796–1801.

[57] Y. Liu, W. Cheng, S. Guilley, and O. Rioul, "On conditional alpha-information and its application to side-channel analysis," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Oct. 2021, pp. 1–6.

[58] J. Béguinot, Y. Liu, O. Rioul, W. Cheng, and S. Guilley, "Maximal leakage of masked implementations using Mrs. Gerber's lemma for min-entropy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2023, pp. 654–659.

Atefeh Gilani (Student Member, IEEE) received the B.S. degree in electrical engineering from the K. N. Toosi University of Technology, Iran, in 2016, and the M.S. degree in electrical engineering from the University of Tehran, Iran, in 2019. She is currently pursuing the Ph.D. degree with the School of Electrical, Computer and Energy Engineering, Arizona State University. Her research interests include privacy, information theory, and machine learning.

Gowtham R. Kurri (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the International Institute of Information Technology (IIIT), Hyderabad, India, in 2011, and the M.Sc. and Ph.D. degrees from the Tata Institute of Fundamental Research, Mumbai, India, in 2020.

From 2020 to 2023, he was a Post-Doctoral Researcher with the School of Electrical, Computer and Energy Engineering, Arizona State University. Since February 2023, he has been an Assistant Professor with IIIT Hyderabad, where he is affiliated to the Signal Processing and Communications Research Centre. From 2011 to 2012, he was an Associate Engineer with Qualcomm India Pvt. Ltd., Hyderabad. From July 2019 to October, 2019, he was a Research Intern with the Blockchain Technology Group, IBM Research, Bengaluru, India. His research interests are in information theory and statistical machine learning.

Oliver Kosut (Senior Member, IEEE) received the B.S. degree in electrical engineering and mathematics from Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2004, and the Ph.D. degree in electrical and computer engineering from Cornell University, Ithaca, NY, USA, in 2010.

Since 2012, he has been a Faculty Member with the School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ, USA, where he is an Associate Professor. Previously, he was a Post-Doctoral Research Associate with MIT, from 2010 to 2012. His research interests include information theory, particularly with the applications to security and machine learning and power systems.

Prof. Kosut received the NSF CAREER Award in 2015. He is an Associate Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He has also served as a Co-Lead Editor for an Special Issue on Information-Theoretic Methods for Trustworthy and Reliable Machine Learning for the IEEE JOURNAL ON SELECTED AREAS IN INFORMATION THEORY. He is an IEEE Information Theory Society Distinguished Lecturer, from 2023 to 2024.

Lalitha Sankar (Senior Member, IEEE) received the B.Tech. degree from the Indian Institute of Technology, Bombay, the M.S. degree from the University of Maryland, and the Ph.D. degree from Rutgers University.

She is currently a Professor with the School of Electrical, Computer and Energy Engineering, Arizona State University. Her research interests include applying information theory and data science to study reliable, responsible, and privacy-protected machine learning.

Prof. Sankar received the National Science Foundation CAREER Award in 2014, the IEEE Globecom 2011 Best Paper Award for her work on privacy of side-information in multi-user data systems, and the Academic Excellence Award from Rutgers University in 2008. She is an Associate Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE TRANSACTIONS ON INFORMATION THEORY. She has served as an Associate Editor for *IEEE BITS Magazine*. She has also served as a Co-Lead Editor for a Special Issue on Information-Theoretic Methods for Trustworthy and Reliable Machine Learning for the IEEE JOURNAL ON SELECTED AREAS IN INFORMATION THEORY.

Authorized licensed use limited to: Arizona State University. Downloaded on August 16,2024 at 15:01:21 UTC from IEEE Xplore. Restrictions apply.