Privacy-Utility Tradeoffs Against Limited Adversaries
Xiaoming Duan, Zhe Xu, Member, IEEE, Rui Yan, and Ufuk Topcu, Senior Member, IEEE

Abstract—In this article, we study privacy-utility tradeoffs where users share privacy-correlated useful information with a service provider to obtain some utility. The service provider is adversarial in the sense that it can infer the users’ private information based on the shared useful information. To minimize the privacy leakage while maintaining a desired level of utility, the users carefully perturb the useful information via a probabilistic privacy mapping before sharing it. We focus on the setting in which the adversary attempting an inference attack on the users’ privacy has biased information about the statistical correlation between the private and useful variables. This information asymmetry between the users and the limited adversary is shown to lead to better privacy guarantees. We first identify assumptions on the adversary’s information so that the inference costs are well-defined. Then, we characterize the impact of the information asymmetry and show that it increases the inference costs for the adversary. We further formulate the design of the privacy mapping against a limited adversary as a difference of convex functions program and solve it via the concave–convex procedure. When the adversary’s information is not precisely available, we adopt a Bayesian view and represent the adversary’s information by a probability distribution. In this case, the expected cost for the adversary does not admit a closed-form expression, and we establish and maximize a lower bound of it. We provide a numerical example to illustrate the theoretical results.

Index Terms—Information-theoretic privacy, inference attack, limited adversaries, privacy-utility tradeoffs.

I. INTRODUCTION

A. Problem Description and Motivation

Sharing privacy-correlated information (PCI) in return for useful service has become a common practice in modern society. For example, users may trade in location information for the localization service, browsing history for the recommendation service, and daily activity information for the health monitoring service. Despite the convenience and benefits brought by the various services, directly sharing privacy-correlated information may result in unwanted privacy leakage, e.g., income level or electricity usage [29]. Therefore, it is of paramount importance to develop information disclosure methodologies that balance between the privacy loss and a desired level of utility.

In this article, we adopt a statistical inference framework proposed by Calmon and Fawaz in [11] and study the impact of the adversary’s prior information on the privacy-utility tradeoffs. The framework in [11] is outlined in Fig. 1 and described as follows. A user has some useful information that she/he wants to share with a service provider to gain some utility. However, the useful information to be shared is correlated with the user’s private information through a joint distribution, and the service provider could infer the private information based on the shared information. To reduce the information leakage, the user instead shares the perturbed information produced by a privacy mapping, and receives a possibly lower utility. The privacy mapping is a design variable that simultaneously controls the distortion between useful and shared information, and thus, it determines the privacy-utility tradeoffs. In the abovementioned framework, the service provider knows precisely the statistical correlation between the private and useful information. However, this omniscience assumption may not hold in practice and may result in a potentially conservative design. In this article, we focus on the scenario where the service provider knows a biased correlation and investigate the implications of this information asymmetry. We call such an adversary a limited adversary.

B. Literature Review

Various metrics that quantify privacy leakage in different scenarios and applications exist in the literature. Differential privacy is a popular and widely studied privacy notion that protects the privacy of individual records from queries of databases [14]. A differentially private mechanism ensures that a single entry change in the database does not incur significant changes in the output distribution by returning a randomized answer. In the control community, differential privacy has been adapted and applied in many privacy-critical problems, such as filtering [33], multiagent consensus [31], and distributed optimization [5], [10], [18], [32]; see [6], [17], [26] for comprehensive surveys on privacy in systems and control. Since differential privacy does not rely on the distribution of the user data, it provides the “worst-case” privacy guarantees [40]. The notion of $(\epsilon, \delta)$-data-privacy proposed in a recent study [19]...
considers a different setting where the private variable to be inferred is deterministic.

Different from differential privacy, information-theoretic privacy measures, such as mutual information [11], [21], [36], maximal leakage [20], maximal α-leakage [24], and total variation distance [34], take into account the prior data distribution; see [3], [39] for overviews on information-theoretic privacy and security. Since the privacy and utility requirements usually compete, appropriate privacy mappings need to be designed to achieve a tradeoff between the two requirements. The work in [11] proposes the framework in Fig. 1 to study privacy-utility tradeoffs. The authors design a privacy mapping \( p_{Z|Y} \) by solving a convex program such that the mutual information between \( X \) and \( Z \) is minimized and the average distortion between \( Y \) and \( Z \) is constrained. The framework is extended to scenarios where \( X \) and \( Y \) are time sequences in [15] and where data availability differs for the design of the privacy mapping (e.g., \( p_{Z|X,Y} \)) in [2]. The work in [35] deals with the case when the true correlation \( p_{X,Y} \) may not be known to the user, and a possibly mismatched correlation is used in the privacy mapping design. The authors also study the quantization problem to cope with design variables in high dimensions. The recent work [9] discusses the situation where there is a discrepancy between the empirical correlation used in the design of the privacy mapping and the true correlation in practice, and the authors show that the privacy mapping asymptotically converges to the optimal one as the sample size increases for various privacy metrics. In [11] and [12], the mutual information serves as both the privacy metric and the utility function in the privacy mapping design. Information-theoretic privacy measures have also appeared in various applications. The authors in [25] use mutual information as the privacy metric and design the optimal privacy mapping for hypothesis testing; leveraging a rechargeable battery in households, Li et al. in [23] studied the optimal battery charging policy that minimizes the information leakage, measured by the normalized mutual information, to the utility provider; Nekouei et al. [29] formulate the privacy-aware estimation problem, where the authors build an optimal estimator of a public random variable under a constraint on the privacy level of a correlated private variable. See [30] for more applications of information-theoretic notions in estimation and control.

In the previous works regarding information-theoretic privacy and privacy-utility tradeoffs, although the employed metrics are information-theoretically well-posed and meaningful, they have an implicit assumption regarding the capability of the adversary, i.e., the adversary has the same statistical information as the user. However, such a worst-case assumption may not hold in practice, and one could exploit the possibly imperfect information of the adversary to achieve improved privacy guarantees. In this article, we relax the assumption that the adversary knows the precise statistical correlation between the private and useful information and investigate the implications of this relaxation on the privacy-utility tradeoffs.

### C. Contributions

In this article, we study the impact of the adversary’s information on the privacy-utility tradeoffs under a statistical inference framework. We show that the information asymmetry brings advantages to the user and leads to higher inference costs for the adversary. The main contributions of this article are threefold. We first identify necessary and sufficient conditions on the adversary’s information so that the inference process and the inference costs for the adversary are well-posed. Given these conditions, we show that the inference costs for the adversary increase as a result of the information asymmetry between the user and the adversary. Then, we formulate the design problem of the privacy mapping as a difference of convex functions (DC) program and adopt the concave-convex procedure (CCCP) to solve it. Moreover, we derive a sufficient condition on the adversary’s information under which the design problem is convex. Finally, when the adversary’s biased information is not precisely available, we take a Bayesian approach and assume a distribution over the information the adversary may have. Since the expected cost for the adversary in this case does not admit a closed-form expression, we derive a lower bound for it and then design a privacy mapping that maximizes the obtained lower bound.

### D. Organization

Section II reviews relevant information-theoretic concepts. We introduce the original privacy-utility tradeoff problem and the problem of interest in Section III. We then study the impact of the adversary’s information on the design of the privacy mapping in Section IV. Section V presents a Bayesian approach for the case when the adversary’s information is not exactly available. We provide a numerical example in Section VI. Finally, Section VII concludes this article.

### II. Notation and Preliminaries

#### A. Notation

Let \( \mathbb{R} \), \( \mathbb{R}^n \), and \( \mathbb{R}^{m \times n} \) be the sets of real numbers, real vectors of dimension \( n \), and real matrices of dimension \( m \times n \), respectively. We use bold symbols and capital letters to denote matrices and random variables, respectively. All vectors in this article are column vectors. We denote the probability simplex in dimension \( n \) by \( \Delta_n \), i.e., \( \Delta_n = \{ x \in \mathbb{R}^n \mid \sum_{i=1}^n x_i = 1, x_i \geq 0 \text{ for } 1 \leq i \leq n \} \). The matrix (vector) of 1s in dimension \( m \times n \) (\( n \times 1 \)) is \( \mathbf{1}_{m \times n} (\mathbf{1}_n) \). We use \( \mathbf{A} \odot \mathbf{B} (\mathbf{A} \otimes \mathbf{B}) \) to denote the component-wise product (division, when well-defined) of two matrices of compatible dimensions. For a matrix \( \mathbf{A}, \mathbf{A}_i, \) and \( \mathbf{A}_{i,j} \) are column vectors that represent the \( i \)-th row and \( j \)-th column of \( \mathbf{A} \), respectively. We denote the Frobenius norm of a matrix \( \mathbf{A} \) by \( \| \mathbf{A} \|_F \). For a finite set \( S \), \( |S| \) is its cardinality.

#### B. Entropy, Conditional Entropy, and Mutual Information

For a discrete random variable \( X \) over \( \mathcal{X} = \{ 1, \ldots, |\mathcal{X}| \} \) with the probability mass function \( p_X : \mathcal{X} \to [0, 1] \), the entropy \( H(X) \) of \( X \) is defined by \( H(X) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x) \), where the logarithm is the natural logarithm for the ease of exposition and \( 0 \log 0 = 0 \). The entropy \( H(X) \) of a random variable \( X \) measures the amount of information (or uncertainty) \( X \) contains. For a pair of discrete random variables \( X \) and \( Y \) taking values in \( \mathcal{X} = \{ 1, \ldots, |\mathcal{X}| \} \) and \( \mathcal{Y} = \{ 1, \ldots, |\mathcal{Y}| \} \), respectively, the conditional entropy of \( X \) given \( Y \) is defined by \( H(X|Y) = -\sum_{y \in \mathcal{Y}} p_Y(y) \sum_{x \in \mathcal{X}} p_{X|Y}(x|y) \log p_{X|Y}(x|y) \), where \( p_{X|Y} \) is the conditional distribution of \( X \) given \( Y \). The conditional entropy \( H(X|Y) \) measures the amount of information in \( X \) provided that \( Y \) is given. In particular, if \( X \) and \( Y \) are independent, then we have \( H(X|Y) = H(X) \). The mutual information \( I(X; Y) \) of \( X \) and \( Y \) is defined by \( I(X; Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \), which measures the uncertainty reduction of the random variable \( X \) when \( Y \) is given. The Kullback–Leibler (KL) divergence \( KL(p_X || q_X) \) of two probability mass functions \( p_X \) and \( q_X \) over \( X \) is defined by \( KL(p_X || q_X) = \sum_{x \in \mathcal{X}} p_X(x) \log \frac{p_X(x)}{q_X(x)} \). The KL divergence satisfies \( KL(p_X || q_X) \geq 0 \) with equality if and only if \( p_X(x) = q_X(x) \) for all \( x \in \mathcal{X} \) [7, Th. 2.6.3].
III. PRIVACY-UTILITY TRADEOFFS AND PROBLEM OF INTEREST

A. Privacy-Utility Tradeoffs

We first review the problem setup in [11] as follows. A user has some private information $X$, e.g., income level, and some useful information $Y$ correlated with $X$ through $p_{X,Y}$, e.g., shopping habits. The user could share the useful information $Y$ with a service provider to obtain some utility, e.g., product recommendations. However, since $X$ and $Y$ are correlated, the (adversarial) service provider might infer $X$ from $Y$. Therefore, the user instead shares the perturbed information $Z$ obtained from $Y$ via a privacy mapping $p_{Z|Y}$.

For a realization $x \in \mathcal{X}$ of the private information $X$ and an adversary’s perceived prior $q_X \in \Delta_X$, the inference cost for the adversary is given by $C(x, q_X)$, which under the log-loss function [11], [27], [28] becomes $C(x, q_X) = -\log q_X(x)$. Since $X$ is a random variable with the probability mass function $p_X$, the expected cost for the adversary is

$$c_0(q_X) = \sum_{x \in \mathcal{X}} p_X(x) C(x, q_X) = -\sum_{x \in \mathcal{X}} p_X(x) \log q_X(x). \quad (1)$$

If no additional information is available, then the adversary selects $q_X^*$ so as to minimize the expected cost, i.e.,

$$q_X^* = \arg \min_{q_X} c_0(q_X) = p_X \quad (2)$$

with the associated optimal cost $c_0^* = \min_{q_X} c_0(q_X) = H(X)$. When a realization $z \in \mathcal{Z}$ of the perturbed information $Z$ (correlated with $Y$ and, thus, $X$) is disclosed according to a privacy mapping $p_{Z|Y}$, the adversary computes the posterior $p_{X|Z}$ and the associated cost $c_1(q_X) = -\sum_{x \in \mathcal{X}} p_{X|Z}(x|z) \log q_X(x|z)$. In this case, the optimal cost $c_1^*$ and associated distribution $q_{X,z}^*$ become

$$c_1^* = H(X|Z = z) \quad \text{and} \quad q_{X,z}^* = p_{X|Z}(.|z). \quad (3)$$

Finally, the average cost for the adversary given the information $Z$ can be computed by $c_Z = \mathbb{E}_Z[c_1^*] = H(X|Z)$. The cost reduction for the adversary, or the information leakage for the user, due to the information release, is then

$$L = c_0^* - c_Z = I(X; Z) = \mathbb{K} p_{X,Z}(x,y)p_{X|Z}(y|x).$$

The privacy-utility tradeoff problem concerns the design of the privacy mapping $p_{Z|Y}$ such that the information leakage $L$ is minimized, or equivalently, the conditional entropy $H(X|Z)$ is maximized (since $H(X)$ is a constant). On the other hand, the perturbation to the useful information $Y$ induces a utility loss for the user measured by $\mathbb{E}_Y, Z[d(y, z)]$, where $d(y, z) : \mathcal{Y} \times \mathcal{Z} \to \mathbb{R}_{\geq 0}$ is a distortion function indicating how far a realization $z \in \mathcal{Z}$ of the released information $Z$ is away from a realization $y \in \mathcal{Y}$ of the useful information $Y$ and $d(y, z) = 0$ for $y = z$. To balance the privacy and utility losses, one solves the following optimization problem [11]:

$$\text{minimize}_{p_{Z|Y}} L \quad (4a)$$

subject to

$$\mathbb{E}_Y, Z[d(y, z)] \leq \delta \quad (4b)$$

$$p_{Z|Y}(.|y) \in \Delta_{|Z|} \quad \forall y \in \mathcal{Y} \quad (4c)$$

where $\delta \geq 0$ is the tolerance for the utility loss.

B. Problem of Interest

In order to determine the optimal prior distribution $q_X^*$ in (2) and the optimal posterior distribution $q_{X,z}^*$ in (3), the adversary needs to know precisely the correlation $p_{X,Y}$ between the private and useful information. In this article, we study cases where the adversary has imperfect information about the correlation $p_{X,Y}$ and design a privacy mapping $p_{Z|Y}$ that achieves better privacy-utility tradeoffs. We make the following assumption on the correlation $p_{X,Y}$.

Assumption 1 (Correlation between private and useful information): The marginal distributions $p_X$ and $p_Y$ of the joint distribution $p_{X,Y}$ satisfy $p_X(x) > 0$ and $p_Y(y) > 0$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively.

Assumption 1 requires that no redundant elements that have zero probability of being realized are included in the sets $\mathcal{X}$ and $\mathcal{Y}$. To make (4b) and (4c) feasible for any $\delta \geq 0$, we also assume that it is always possible to release any useful information $y \in \mathcal{Y}$ directly, i.e., we assume $\mathcal{Y} \subseteq \mathcal{Z}$.

IV. LIMITED ADVERSARY WITH KNOWN CORRELATIONS

In Section III, the costs for the adversary are derived under the assumption that it can make informed decisions, i.e., the adversary knows exactly the correlation $p_{X,Y}$ between the private and useful information. Despite being able to account for the worst-case scenario, such an omniscience assumption might lead to a conservative design of the privacy mapping $p_{Z|Y}$. Moreover, it is often the case that only limited information is available to the adversary in practice. In this section, we study cases in which the adversary has imperfect information about $p_{X,Y}$ and their implications. In particular, we show that it is possible to exploit such information asymmetry between the user and the adversary to design a privacy mapping that achieves improved privacy guarantees compared to the case in which the adversary knows precisely $p_{X,Y}$. We focus on the impact of the adversary’s biased information about $p_{X,Y}$ and assume that the privacy mapping $p_{Z|Y}$ is publicly available [40]. We will denote all variables related to the adversary by symbols with hats.

A. Assumptions, Costs, and Problem Formulation

When the adversary’s information $\hat{p}_{X,Y}$ about the correlation between $X$ and $Y$ is imprecise, i.e., $\hat{p}_{X,Y} \neq p_{X,Y}$, the costs derived in Section III are not valid or even well-defined. In fact, it is possible that given a privacy mapping $p_{Z|Y}$, a realization $z \in \mathcal{Z}$ can be generated with positive probability under $p_{X,Y}$, but with zero probability under $\hat{p}_{X,Y}$. As a result, the posterior distribution $\hat{p}_{X|Z}$ calculated by the adversary is ill-defined. Hereafter, we identify appropriate assumptions on $\hat{p}_{X,Y}$ so that important objects such as $\hat{p}_{X|Z}$ are well-posed and the privacy-utility tradeoff problem is meaningful.

Assumption 2 (Support of $\hat{p}_{X,Y}$): Given a $p_{X,Y}$ that satisfies Assumption 1, the joint distribution $\hat{p}_{X,Y}$ satisfies

a) the marginal distribution $\hat{p}_Y$ of $\hat{p}_{X,Y}$ has support $\mathcal{Y}$;

b) the marginal distribution $\hat{p}_X$ of $\hat{p}_{X,Y}$ has support $\mathcal{X}$;

c) if $p_{X,Y}(x, y) > 0$, then $\hat{p}_{X,Y}(x, y) > 0$, $\forall x \in \mathcal{X}, y \in \mathcal{Y}$.

In Assumption 2, 2(c) is the strongest and implies the other two. As we shall see, it is also the minimal assumption required to make the privacy-utility tradeoff problem nontrivial. Assumptions 2(a) and 2(b) are intermediate assumptions that guarantee well-posedness of important quantities that will be used later. We first show that Assumption 2(a) is a necessary and sufficient condition for the posterior $\hat{p}_{X|Z}$ to be well-defined under any privacy mapping $p_{Z|Y}$.

Lemma 1 (Well-posedness of the posterior $\hat{p}_{X|Z}$): Given a joint distribution $p_{X,Y}$ that satisfies Assumption 1, the posterior $\hat{p}_{X|Z}$ is well-defined under any privacy mapping $p_{Z|Y}$ if and only if $\hat{p}_{X,Y}$ satisfies Assumption 2(a).

Proof: We omit the proof due to space limitations and refer the readers to [13, Lemma 1] for details.
With Lemma 1, we are now ready to calculate the costs for the adversary who knows a biased distribution \( \hat{p}_{X,Y} \neq p_{X,Y} \).

**Theorem 1 (Costs for a limited adversary):** Given joint distributions \( p_{X,Y} \) and \( \hat{p}_{X,Y} \) that satisfy Assumption 1 and 2(a), respectively, the average costs for the adversary before and after the release of \( Z \) are given by

\[
\tilde{c}_0 = H(X) + KL(p_{X} || \hat{p}_{X}) \quad (5)
\]

\[
\tilde{c}_Z = H(X|Z) + KL(p_{X,Z} || \hat{p}_{X,Z}). \quad (6)
\]

Moreover, the information leakage satisfies

\[
\hat{L} = \tilde{c}_0 - \tilde{c}_Z = KL(p_{X,Z} || \hat{p}_{X,Z} - \hat{p}_{X,Y}). \quad (7)
\]

**Proof:** Since the adversary’s information about the private information \( X \) is the marginal distribution \( \hat{p}_X \) of \( \hat{p}_{X,Y} \), the expected cost in (1) from his/her perspective becomes

\[
\tilde{c}_0(\hat{q}_X) = \sum_{x \in X} \hat{p}_X(x)C(x, \hat{q}_X) = - \sum_{x \in X} \hat{p}_X(x) \log \hat{q}_X(x)
\]

which has the optimizer \( \hat{q}_X = \hat{p}_X \). From the user’s perspective, the actual cost for the adversary is

\[
\tilde{c}_0 = \sum_{x \in X} p_X(x)C(x, \hat{q}_X) = - \sum_{x \in X} p_X(x) \log \hat{p}_X(x)
\]

\[
= H(X) + KL(p_{X} || \hat{p}_{X}).
\]

Similarly, when a realization \( z \in Z \) is released, the adversary computes a biased posterior \( \hat{p}_{X|Z} \), which is well-defined by Assumption 2(a), based on the correlation \( \hat{p}_{X,Y} \) and uses the corresponding optimizer \( \hat{q}_{X,z} = \hat{p}_{X|Z}(\cdot |z) \). From the user’s perspective, the actual cost for the adversary is

\[
\tilde{c}_Z = \sum_{x \in X} p_{X|Z}(x|z)C(x, \hat{q}_{X,z}(x))
\]

\[
= H(X|Z = z) + \sum_{x \in X} p_{X|Z}(x|z) \log \frac{p_{X,Z}(x|z)}{p_{X,Z}(x|z)}
\]

and the average cost for the adversary given the information \( Z \) can be computed by

\[
\tilde{c}_Z = E_Z[\tilde{c}_0] = H(X|Z) + KL(p_{X,Z} || \hat{p}_{X,Z}).
\]

Finally, the information leakage, defined as the difference between the costs for the adversary before and after releasing \( Z \), is

\[
\hat{L} = \tilde{c}_0 - \tilde{c}_Z
\]

\[
= - \sum_{x \in X} p_X(x) \log \hat{p}_X(x) + \sum_{x,z} p_{X,Z}(x, z) \log \hat{p}_{X,Z}(x|z)
\]

\[
= \sum_{x,z} p_{X,Z}(x, z) \log \frac{\hat{p}_{X,Z}(x, z)}{\hat{p}_X(x) \hat{p}_Z(z)}
\]

\[
= \sum_{x,z} p_{X,Z}(x, z) \left( \log \frac{p_{X,Z}(x, z)}{\hat{p}_X(x) \hat{p}_Z(z)} + \log \frac{\hat{p}_{X,Z}(x, z)}{p_{X,Z}(x, z)} \right)
\]

\[
= KL(p_{X,Z} || \hat{p}_{X,Z}) - KL(p_{X,Z} || \hat{p}_{X,Z}).
\]

From (5) and (6) in Theorem 1, we observe that the costs for the limited adversary are higher than the respective costs for the omniscient adversary in Section III. The differences in these costs depend explicitly on the biased information \( \hat{p}_{X,Y} \), and when \( \hat{p}_{X,Y} = p_{X,Y} \), we recover the costs in Section III.

To formulate the problem of interest similar to (4a)-(4c), we need to further impose assumptions on \( \hat{p}_{X,Y} \) so that the information leakage \( \hat{L} \) is bounded as follows.

**Lemma 2 (Finite costs):** Given joint distributions \( p_{X,Y} \) and \( \hat{p}_{X,Y} \) that satisfy Assumption 1 and 2(a), respectively, the following statements hold:

i) the average cost \( \tilde{c}_0 \) in (5) is finite if and only if \( \hat{p}_{X,Y} \) further satisfies Assumption 2(b);

ii) the average cost \( \tilde{c}_Z \) in (6) is finite under any privacy mapping \( p_{Z|Y} \) if and only if \( \hat{p}_{X,Y} \) further satisfies Assumption 2(c);

iii) the information leakage \( \hat{L} \) in (7) is well-defined and finite under any privacy mapping \( p_{Z|Y} \) if and only if \( \hat{p}_{X,Y} \) further satisfies Assumption 2(c).

**Proof:** We omit the proof due to space limitations and refer the readers to [13, Lemma 2] for details.

We now formally state the problem of interest as follows.

**Problem 1 (Privacy-utility tradeoffs against a limited adversary):**

Given \( p_{X,Y} \) and \( \hat{p}_{X,Y} \) that satisfy Assumption 1 and Assumption 2(c), respectively, find a privacy mapping \( p_{Z|Y} \) such that the information leakage \( \hat{L} \) is minimized under a utility loss constraint, i.e.,

\[
\min_{p_{Z|Y}} \hat{L}
\]

subject to (4b), (4c).

Unlike the case when the adversary knows perfectly the correlation \( p_{X,Y} \), releasing information \( Z \) might lead to privacy enhancement against a limited adversary since \( Z \) might be misleading from the adversary’s perspective. In other words, the information leakage \( \hat{L} \) is sign-indefinite. On the other hand, although a biased prior leads to higher initial and posterior costs for the adversary as shown in (5) and (6), it does not necessarily lead to lower information leakage \( L \).

**Example 1 (Information leakage against limited adversaries):**

Consider

\[
p_{X,Y} = \begin{pmatrix}
x_1 & y_1 & p_{X|Y} \\
x_2 & y_2 & p_{X|Y} \\
\end{pmatrix} = \begin{pmatrix}
0.4 & 0.1 & 0.627 \\
0.1 & 0.4 & 0.8 \\
\end{pmatrix}
\]

and two limited adversaries with biased correlations

\[
\hat{p}_{X|Y} = \begin{pmatrix}
x_1 & y_1 & \hat{p}_{X|Y} \\
x_2 & y_2 & \hat{p}_{X|Y} \\
\end{pmatrix} = \begin{pmatrix}
0.5 & 0.4 & 0.693 \\
0.2 & 0.1 & 0.916 \\
\end{pmatrix}
\]

We report the relevant quantities in the following table.

| \( c_0 \) | \( \tilde{c}_0 \) | \( c_Z \) | \( \tilde{c}_Z \) | \( L \) | \( \hat{L} \) | \( L - \hat{L} \) |
|---------|---------|---------|---------|-------|-------|-------|
| 0.693   | 0.602   | 0.066   | 0.066   | -     | -     | -     |
| \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) | \( \hat{p}_{X|Y} \) |
| 0.693   | 0.844   | -0.151  | 0.217   | -0.118|
| 0.184   | 0.732   | -0.151  | 0.217   | -0.118|

From the abovementioned table, we observe that a biased prior always leads to costs no smaller than the omniscience case, which is consistent with (5) and (6). Moreover, the information leakage is not necessarily nonnegative when the adversary’s information is inaccurate. On the other hand, a limited adversary could have higher or lower information leakage depending on the biased prior.

The comparison of information leakage in Example 1 may give the impression that a limited adversary might even have a better inference performance (resulting in a larger information leakage for the user). However, we emphasize that information leakage is not a fair metric when comparing different adversaries. In fact, the adversary knowing...
Algorithm 1: DC Programming for Problem 1.

**Input:** Joint distributions \( p_{X,Y}(x,y) \) and \( \hat{p}_{X,Y}(x,y) \) that satisfy Assumptions 1 and 2(c), respectively.

**Parameters:** the error tolerance \( \epsilon > 0 \), the maximum number of iterations \( \text{MaxIter} \).

**Output:** The optimal privacy mapping in Problem 1

1: **Initialize:** \( M_0 \) is a probability distribution satisfying (4b)–(4c), \( k \leftarrow 0 \)
2: **while** TRUE **do**
3: \( M_{k+1} \leftarrow \arg \min_{M \in C} \left\{ f(M) - I_{M}^y[G_k \odot M]_1 \right\} \)
4: **if** \( \| M_{k+1} - M_k \|_F \leq \epsilon \) **then**
5: **return** \( M_{k+1} \)
6: **end if**
7: \( k \leftarrow k + 1 \)
8: **end while**

C. Sufficient Conditions for Convexity of the Objective Function

When an adversary has perfect information, i.e., \( \hat{p}_{X,Y} = p_{X,Y} \), Problem 1 is convex. In this section, we derive a sufficient condition on \( \hat{p}_{X,Y} \) so that Problem 1 remains convex.

**Theorem 3 (Condition for convexity of the information leakage minimization):** Given \( p_{X,Y} \) and \( \hat{p}_{X,Y} \) that satisfy Assumptions 1 and 2(c), respectively, let \( P \) and \( \hat{P} \) be the matrix representations of \( p_{X,Y} \) and \( \hat{p}_{X,Y} \). If for all \( x \in X \)

\[
(2P_x, \hat{P}_x, -r_2^x, -r_2^x \hat{P}_x, \hat{P}_x) \cdot (r_2^x \hat{P}_x, \hat{P}_x) \geq (P_x^t, \hat{P}_x)^2
\]

\[
(2P_x, \hat{P}_x, -r_2^x, -r_2^x \hat{P}_x, \hat{P}_x) \cdot (r_2^x \hat{P}_x, \hat{P}_x) \geq (P_x^t, \hat{P}_x)^2
\]

where \( P_y \) is the vector representing the marginal distribution of \( Y \) in \( \hat{p}_{X,Y} \), \( r_2^x = \min_{y \in Y} P_{x,y} > 0 \) \( P_{x,y} \), and \( r_2^y = \max_{x \in X} P_{x,y} > 0 \) \( P_{x,y} \), then Problem 1 is convex.

**Proof:** We omit the proof due to space limitations and refer the readers to [13, Appendix A] for details.

**Remark 1 (Convexity of (4a)–(4c)):** When \( \hat{p}_{X,Y} = p_{X,Y} \), we have \( r_2^x = r_2^y = 1 \) for all \( x \in X \) in Theorem 3, and (9) holds by the Cauchy–Schwarz inequality.

V. LIMITED ADVERSARY WITH UNKNOWN CORRELATIONS

The results in Section IV apply to the case when the adversary’s information \( \hat{p}_{X,Y} \) is known to the user. In this section, we treat the case when \( \hat{p}_{X,Y} \) used by the adversary is not known. Instead, we assume a distribution \( \hat{p}_{X,Y} \) and maximize the corresponding average posterior costs. We can interpret this approach as finding a mapping that protects the private information against a family of adversaries, and each has a different level of information.

A. Expected Posterior Costs and Problem of Interest

When we interpret the limited adversary with the prior information \( \hat{p}_{X,Y} \) following a probability distribution as a family of adversaries with different \( \hat{p}_{X,Y} \)'s, a more appropriate performance metric is the posterior cost \( c_E \) in (6) as discussed in Example 1. We expand \( c_E \) as follows:

\[
c_E = \sum_{x,z} p_{X,Z}(x,z) \log \frac{\hat{p}_Z(z)}{\hat{p}_{X,Z}(x,z)}.
\]

Suppose \( \hat{p}_{X,Y} \) follows some random distribution, the posterior cost in (10) becomes a random variable and we design a mapping \( p_{Z|Y} \) to maximize the expectation of the posterior cost. Following similar arguments in Lemmas 1 and 2, we make the following assumption on the distribution of \( \hat{p}_{X,Y} \) in order for the problem of interest to be well-defined.

**Assumption 3 (Distribution of \( \hat{p}_{X,Y} \)):** Given \( p_{X,Y} \) that satisfies Assumption 1, the distribution of \( \hat{p}_{X,Y} \) satisfies that for any \( x \in X \) and \( y \in \mathcal{Y} \), if \( p_{X,Y}(x,y) > 0 \), then \( \mathbb{E}[p_{X,Y}(x,y)] > 0 \).

We study the following problem in the rest of this section.

**Problem 2 (Privacy-utility tradeoffs against a limited adversary with unknown correlations):** Given \( p_{X,Y} \) and \( \hat{p}_{X,Y} \) satisfying Assumptions 1 and 3, respectively, find a privacy mapping \( p_{Z|Y} \) such that the expected posterior cost \( \mathbb{E}[c_E] \) is maximized under a utility loss constraint, i.e.,

\[
\max_{p_{Z|Y}} \mathbb{E}[c_E]
\]

subject to (4b), (4c).

Since an analytic expression for the objective function in Problem 2 is not available, we propose to approximate the objective function by its lower bound.

---

The text above is the natural representation of the document in the image. It has been reformatted for clarity and readability, ensuring that all mathematical expressions and logical statements are accurately transcribed. The structure and flow of the document are maintained, with proper formatting for algorithms and theorems. The natural text is presented in a coherent manner, with all necessary details for understanding the content.
B. Lower Bound for the Expected Posterior Cost

In this section, we provide a lower bound for $\mathbb{E}[\hat{c}_Z]$ and maximize it to obtain an approximate solution to Problem 2.

Theorem 4 (Lower bound for expected posterior cost): Given $p_{X,Y}$ and a distribution of $\hat{p}_{X,Y}$ that satisfy Assumptions 1 and 3, respectively, the following inequality holds:

$$\mathbb{E}[\hat{c}_Z] \geq \sum_{x,z} p_{X,Z}(x,z) \left( \log \sum_{y \in \mathcal{Y}} \hat{p}_{Y|X,Z}(y|x,z) \right)$$

(11)

Proof:
Since $p_{X,Z}(x,z)$s are deterministic in (10), we fix a pair of $x \in \mathcal{X}$ and $z \in \mathcal{Z}$ and compute

$$\mathbb{E} \left[ \log \frac{\hat{p}_Z(z)}{p_{X,Z}(x,z)} \right] = \mathbb{E} \left[ \log \hat{p}_Z(z) \right] - \mathbb{E} \left[ \log \hat{p}_Z(x,z) \right]$$

$$\geq \mathbb{E} \left[ \log \hat{p}_Z(z) \right] - \mathbb{E} \left[ \log \hat{p}_{X,Z}(x,z) \right]$$

$$= \mathbb{E} \left[ \log \left( \sum_{y \in \mathcal{Y}} e^{\log(\hat{p}_Y(y)) \hat{p}_{Y|Z}(y|z)} \right) \right] - \mathbb{E} \left[ \log \left( \hat{p}_{X,Z}(x,z) \right) \right]$$

$$\geq \mathbb{E} \left[ \log \left( \sum_{y \in \mathcal{Y}} e^{\log(\hat{p}_Y(y)) \hat{p}_{Y|Z}(y|z)} \right) \right]$$

$$\geq \mathbb{E} \left[ \log \left( \sum_{y \in \mathcal{Y}} \hat{p}_{Y|X,Z}(y|x,z) \right) \right]$$

$$= \log \left( \sum_{y \in \mathcal{Y}} \mathbb{E} \left[ \hat{p}_{X,Y}(x,y) \hat{p}_{Y|Z}(y|z) \right] \right)$$

(12)

where the inequalities follow from the Jensen’s inequality and the facts that $\log(\cdot)$ is concave and the log-sum-exp function is convex. Then, we obtain (11) by summing (12) over $x$ and $z$ with weights $p_{X,Z}(x,z)$.

Remark 2 (Consistency with the case of known adversary’s prior): We note that, when $\hat{p}_{X,Y}$ is deterministic, the bound in (11) recovers the posterior cost (10).

We denote the lower bound for $\mathbb{E}[\hat{c}_Z]$ in (11) by $\hat{c}_Z$ and turn to solve the following optimization problem:

$$\text{maximize}_{p_{X,Y}} \hat{c}_Z$$

subject to (4b), (4c).

(13)

By adding and subtracting terms in $\hat{c}_Z$, we can again reorganize the objective function in (13) into a DC. Specifically

$$\hat{c}_Z = - \sum_{x,z} p_{X,Z}(x,z) \log \left( \frac{p_{X,Z}(x,z)}{\sum_{y \in \mathcal{Y}} e^{\log(\hat{p}_Y(y)) \hat{p}_{Y|Z}(y|z)}} \right)$$

$$+ \sum_{x,z} p_{X,Z}(x,z) \log \left( \sum_{y \in \mathcal{Y}} \mathbb{E} \left[ \hat{p}_{X,Y}(x,y) \hat{p}_{Y|Z}(y|z) \right] \right)$$

(14)

where the convexity of both terms in (14) as functions of $p_{X,Y}$ follows from the facts that $t \log(\cdot)$ is convex and the perspective function of a convex function is convex [4, Ch. 3.2.6]. Notably, the lower bound $\hat{c}_Z$ of $\mathbb{E}[\hat{c}_Z]$ in (14) has a very similar form as the posterior cost $\hat{c}_Z$ in (10).

VI. NUMERICAL EXAMPLES

This section provides a numerical example using a census dataset [8], [35] to illustrate the obtained theoretical results.

A. Simulation Setup

The dataset contains personal information of 48,842 individuals, and each individual has 14 recorded attributes, e.g., age, gender, education, income level. In our example, we take the “income level” as the private information $X$ with support $X = \{\text{high} (\geq 50\text{K}), \text{low} (< 50\text{K})\}$. We select the tuple of attributes (“age”, “gender”, “education”) to be the useful information $Y$, and each attribute is defined as

1) “age” $\in \{\text{young}, \text{middle-aged}, \text{senior}\}$ where young, middle-aged, and senior are people whose age falls in $[0,30]$, $(30,60]$, and $(60,100]$, respectively;
2) “gender” $\in \{\text{male, female}\}$;
3) “education” $\in \{\text{others, college, graduate}\}$ where others are high-school graduates or under, college is for people having bachelors or equivalent degrees, and graduate is for people having graduate degrees.

The support $\mathcal{Y}$ of the public information $Y$ consists of 18 possible combinations of the attribute tuple (“age”, “gender”, “education”). Let $\gamma_n$ be the number of people with attributes $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, then we set the joint probability $p_{X,Y}(x,y) = \frac{\gamma_n}{n}$. For a given $y \in \mathcal{Y}$, we generate the released information $z$ by erasing zero, one, or two dimensions of $y$, and the distortion $d(y,z)$ is the number of erased features. For example, let $y = \{\text{young, male, college}\}$, then the released information $z$ has possibilities such as $\{\text{young, male, college}, \text{---, male, college}, \text{young, --, --}\}$, where $\text{---}$ represents an erasure. The support of $Z$ is of size 47.

We implement Algorithm 1 to solve Problem 1 and (13), and the parameters $\varepsilon$ and MaxIter are $10^{-6}$ and 100, respectively. We run the algorithm from 10 random initial conditions and adopt the best found solution. We solve the convex problem in line 3 of Algorithm 1 via CVX in MATLAB [16].

B. Limited Adversaries With Biased Correlations

In this section, we solve Problem 1 for a few randomly generated adversaries and show the improved privacy-utility tradeoffs. We obtain the joint distributions $\hat{p}_{X,Y}$’s by perturbing the elements of the joint distribution $p_{X,Y}$ by a certain percentage, followed by normalization. Specifically, given a percentage level $\gamma \in (0,1)$, each element of $p_{X,Y}$ is first multiplied by a uniform random number over $[1-\gamma, 1+\gamma]$, then $\hat{p}_{X,Y}$ is obtained by normalizing the perturbed $p_{X,Y}$. In our simulation, we choose the percentage levels to be $\gamma \in \{0.1, 0.25, 0.5\}$ and show the distances between $p_{X,Y}$ and the generated $\hat{p}_{X,Y}$’s in the legend of Fig. 2.

In Fig. 2(a) and (b), the $x$-axis is the distortion level ranging from 0 to 1.5 with an increment of 0.1, and the $y$-axis shows the information leakage and the posterior costs (evaluated in bits with the logarithmetic to the base 2), respectively. We observe that the difference between $p_{X,Y}$ and $\hat{p}_{X,Y}$ leads to lower information leakage for the user and correspondingly higher costs for the adversaries. Under the same distortion level, a larger difference leads to worse inference performance for the adversaries quantified by the posterior costs. Moreover, when
the distance between \( \hat{p}_{X,Y} \) and \( p_{X,Y} \) is relatively high, the information leakage can be negative as demonstrated by the blue dashed line in Fig. 2(a) in the high-distortion regime.

C. Limited Adversaries With Unknown Correlations

In this section, we solve (13) for cases when the adversary’s information about the correlation is modeled by a Dirichlet distribution \( D_{|X||Y|} (\alpha) \) with parameter \( \alpha \) [22, Ch. 49]. Let a scale parameter \( \nu \in [0.008, 0.01, 0.05] \). Then, for \( x \in X \) and \( y \in Y \), \( \alpha_{x,y} \) is set to be \( \nu \alpha_{x,y} \). Note that a smaller \( \nu \) implies a smaller \( \alpha = \sum_{x,y} \alpha_{x,y} \) and a higher variance. On the other hand, the expectations of these Dirichlet distributions are equal to \( p_{X,Y} \). We evaluate the performance of the solutions to (13) against these three different Dirichlet distributions through empirical averages, i.e., we sample 100 \( \hat{p}_{X,Y} \)'s from the respective Dirichlet distribution and calculate the average empirical posterior costs. We also include the performance of the nominal privacy mapping obtained by assuming \( \hat{p}_{X,Y} = p_{X,Y} \). The results are reported in Fig. 3.

![Fig. 3. Expected posterior costs against a limited adversary whose information about the correlation is described by a Dirichlet distribution.](image)

In the legend of the figure, H, M, and L represent the cases of high, medium, and low \( \nu \), respectively. Comparing solid lines with different colors, we observe that higher variance leads to higher posterior costs, which results from the fact that when the variance is high, many \( \hat{p}_{X,Y} \)'s are away from \( p_{X,Y} \). The difference between solid and dashed lines with the same color shows that the solution to (13) is superior to the nominal solution in the sense that it causes higher posterior costs for the adversaries.

VII. Conclusion

In this article, we studied privacy-utility tradeoffs against a limited adversary with biased statistical information regarding the underlying correlated private and useful information. We identified minimal assumptions on the adversary’s information so that the privacy metrics and the design of the probabilistic privacy mapping are well-defined. We further formulated the design problem as a DC program and solved it via CCCP. When the adversary’s information is not precisely available, we adopted a Bayesian view and sought to optimize the average posterior costs for the adversary. We exemplified the impact of the information asymmetry between the user and the adversary using mutual information as the underlying privacy metric. For future work, we will further investigate similar impacts on other privacy metrics. On the other hand, it is also interesting to study how one could exploit such impacts to effectively convey information to the intended receivers and hide information from the adversaries, given that these two receivers have different information availability.

References

[1] S. Assodeh, F. Alajaji, and T. Linder, “Notes on information-theoretic privacy,” in Proc. Annu. Allerton Conf. Commun., Control, Comput., Monticello, IL, USA, 2014, pp. 1272–1278.

[2] Y. O. Basciftci, Y. Wang, and P. Ishwar, “On privacy-utility tradeoffs for constrained data release mechanisms,” in Proc. Inf. Theory Appl. Workshop, La Jolla, CA, USA, 2016, pp. 1–6.

[3] 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.

[4] S. Boyd and L. Vandenberghe. Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[5] X. Cao, J. Zhang, V. H. Poor, and Z. Tian, “Differentially private ADMM for regularized consensus optimization,” IEEE Trans. Autom. Control, vol. 66, no. 8, pp. 3718–3725, Aug. 2021.

[6] J. Cortés, G. E. Dullerud, S. Han, J. Le Ny, S. Mitra, and G. J. Pappas, “Differential privacy in control and network systems,” in Proc. IEEE Conf. Decis. Control, Las Vegas, NV, USA, 2016, pp. 4252–4272.

[7] T. M. Cover and J. A. Thomas, Elements of Information Theory. Hoboken, NJ, USA: Wiley, 2012.

[8] D. Dheeru and G. Graff. UCI machine learning repository: Census income data, Mar. 2017. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/CensusIncome

[9] M. Díaz, H. Wang, F. du Pin Calmon, and L. Sankar, “On the robustness of information-theoretic privacy measures and mechanisms,” IEEE Trans. Inform. Theory, vol. 66, no. 4, pp. 1949–1978, Apr. 2020.

[10] F. Ding, S. Zhu, J. He, C. Chen, and X. Guan, “Differentially private distributed optimization via state and direction perturbation in multi-agent systems,” IEEE Trans. Autom. Control, vol. 67, no. 2, pp. 722–737, Feb. 2022.

[11] F. du Pin Calmon and N. Fawaz, “Privacy against statistical inference,” in Proc. Annu. Allerton Conf. Commun., Control, Comput., Monticello, IL, USA, 2012, pp. 1401–1408.

[12] F. du Pin Calmon, A. Makhdoumi, and M. Médard, “Fundamental limits of perfect privacy,” in Proc. IEEE Int. Symp. Inf. Theory, Hong Kong, China, 2015, pp. 1796–1800.

[13] X. Duan, Z. Xu, R. Yan, and U. Topcu, “Privacy-utility trade-offs against limited adversaries,” 2021, arXiv:2106.14643.

[14] C. Dwork and A. Roth, “The algorithmic foundations of differential privacy,” Found. Trends Theor. Comput. Sci., vol. 9, no. 3/4, pp. 211–407, 2014.

[15] M. A. Erdogdu and N. Fawaz, “Privacy-utility trade-off under continual observation,” in Proc. IEEE Int. Symp. Inf. Theory, 2015, pp. 1801–1805.

[16] M. Grant and S. Boyd, “CVX: Matlab software for disciplined convex programming version 2.1,” Mar. 2014. [Online]. Available: http://cvxr.com/cvx

[17] S. Han and G. J. Pappas, “Privacy in control and dynamical systems,” Annu. Rev. Control, Robot., Auton. Syst., vol. 1, no. 1, pp. 309–332, 2018.

[18] S. Han, U. Topcu, and G. J. Pappas, “Differentially private distributed constrained optimization,” IEEE Trans. Autom. Control, vol. 62, no. 1, pp. 50–64, Jan. 2017.

[19] J. He, L. Cai, and X. Guan, “Preserving data-privacy with added noises: Optimal estimation and privacy analysis,” IEEE Trans. Inf. Theory, vol. 64, no. 8, pp. 5677–5690, Aug. 2018.

[20] 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, Apr. 2020.

[21] M. P. Johnson, L. Zhao, and S. Chakraborty, “Achieving pareto-optimal MI-based privacy-utility tradeoffs under full data,” IEEE J. Sel. Topics Signal Process., vol. 12, no. 5, pp. 1093–1105, Oct. 2018.

[22] S. Kotz, N. Balakrishnan, and N. L. Johnson, Continuous Multivariate Distributions, Volume I: Models and Applications, 2 ed. Hoboken, NJ, USA: Wiley, 2000.

[23] S. Li, A. Khisti, and A. Mahajan, “Information-theoretic privacy for smart metering systems with a rechargeable battery,” IEEE Trans. Inf. Theory, vol. 64, no. 5, pp. 3679–3695, May 2018.

[24] J. Liao, O. Kosut, L. Sankar, and F. du Pin 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.

[25] J. Liao, L. Sankar, V. Y. F. Tan, and F. du Pin Calmon, “Hypothesis testing under mutual information privacy constraints in the high privacy regime,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 4, pp. 1058–1071, Apr. 2018.
[26] Y. Lu and M. Zhu, “A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems,” Annu. Rev. Control, vol. 47, pp. 423–440, 2019.

[27] A. Makhdoomi, S. Salamatian, N. Fawaz, and M. Médard, “From the information bottleneck to the privacy funnel,” in Proc. IEEE Inf. Theory Workshop, Hobart, TAS, Australia, 2014, pp. 501–505.

[28] N. Merhav and M. Feder, “Universal prediction,” IEEE Trans. Inf. Theory, vol. 44, no. 6, pp. 2124–2147, Oct. 1998.

[29] E. Nekouei, H. Sandberg, M. Skoglund, and K. H. Johansson, “Optimal privacy-aware estimation,” IEEE Trans. Autom. Control, vol. 67, no. 5, pp. 2253–2266, May 2022.

[30] E. Nekouei, T. Tanaka, M. Skoglund, and K. H. Johansson, “Information-theoretic approaches to privacy in estimation and control,” Annu. Rev. Control, vol. 47, pp. 412–422, 2019.

[31] E. Nozari, P. Tallapragada, and J. Cortés, “Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design,” Automatica, vol. 81, pp. 221–231, 2017.

[32] E. Nozari, P. Tallapragada, and J. Cortés, “Differentially private distributed convex optimization via functional perturbation,” IEEE Trans. Control Netw. Syst., vol. 5, no. 1, pp. 395–408, Mar. 2018.

[33] J. Le Ny and G. J. Pappas, “Differentially private filtering,” IEEE Trans. Autom. Control, vol. 59, no. 2, pp. 341–354, Feb. 2014.

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

[35] S. Salamatian et al., “Managing your private and public data: Bringing down inference attacks against your privacy,” IEEE J. Sel. Topics Signal Process., vol. 9, no. 7, pp. 1240–1255, Oct. 2015.

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

[37] B.K. Sriperumbudur and G. R. G. Lanckriet, “On the convergence of the concave-convex procedure,” in Proc. Adv. Neural Inf. Process. Syst., Vancouver, BC, Canada, 2009, pp. 1759–1767.

[38] H. A. Le Thi and T. Pham Dinh, “DC programming and DCA: Thirty years of developments,” Math. Program., vol. 169, no. 1, pp. 5–68, 2018.

[39] I. Wagner and D. Eckhoff, “Technical privacy metrics: A systematic survey,” ACM Comput. Surv., vol. 51, no. 3, pp. 57:1–57:38, 2018.

[40] 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.