Asymmetric Local Information Privacy and the Watchdog Mechanism

Mohammad Amin Zarrabian  
*College of Engineering and Computer Science, Australian National University, Canberra, Australia.*  
mohammad.zarrabian@anu.edu.au

Ni Ding  
*School of Computing and Information Systems, University of Melbourne, Melbourne, Australia.*  
ni.ding@unimelb.edu.au

Parastoo Sadeghi  
*School of Engineering and Information Technology, University of New South Wales, Canberra, Australia.*  
p.sadeghi@unsw.edu.au

**Abstract**—This paper proposes a novel watchdog privatization scheme by generalizing local information privacy (LIP) to enhance data utility. To protect the sensitive features $S$ correlated with some useful data $X$, LIP restricts the lift, the ratio of the posterior belief to the prior on $S$ after and before accessing $X$. For each $x$, both maximum and minimum lift over sensitive features quantify the privacy risk of publishing this symbol and should be restricted for the privacy-preserving purpose. Previous works enforce the same bound for both max-lift and min-lift. However, empirical observations show that the min-lift is usually much smaller than the max-lift. In this work, we generalize the LIP definition to consider the unequal values of max and min lift, i.e., considering different bounds for max-lift and min-lift. This new definition is applied to the watchdog privacy mechanism. We demonstrate that the utility is enhanced under a given privacy constraint on local differential privacy. At the same time, the resulting max-lift is lower and, therefore, tightly restricts other privacy leakages, e.g., mutual information, maximal leakage, and $\alpha$-leakage.

**Index Terms**—Local information privacy, Local differential privacy, the Watchdog privacy mechanism.

### I. INTRODUCTION

Today, many businesses and government agencies gather and share massive amounts of data to achieve economic and social benefits through the widespread advancement of communication systems and machine learning algorithms. This phenomenon raises a growing concern about the privacy of individual users that could be at risk by inferring confidential information from datasets explicitly or implicitly. This situation motivates research to design privacy-preserving mechanisms that, besides protecting confidential features, also provide a satisfactory data utility.

The information-theoretic (IT) paradigm measures privacy as information leakage about private data $S$ when correlated useful data $X$ is accessed. In this regard, the lift is a symbol-wise metric of the privacy [1], [2], which determines the adversary’s knowledge gain via measuring the multiplicative gain of posterior belief $P_{S|X}(s|x)$ compared to the prior $P_S(s)$, and is given by:

$$ \ell(s, x) = \frac{P_{S|X}(s|x)}{P_S(s)}. \quad (1) $$

The logarithm of the lift is called log-lift and denoted by $i(s, x) = \log \ell(s, x)$. Lift and log-lift provide strong notions of IT privacy in local information privacy (LIP) [1]–[11], where a sanitized version of $X$ is published to restrict $|i(s, x)|$ below a given threshold $\varepsilon$ known as privacy budget. $\varepsilon$-LIP upper bounds IT measures including the mutual information (MI) [1], [12], maximal leakage [13], $\alpha$-leakage, $\alpha$-lift [14], and Sibson MI [14]–[16]. It also provides a $2\varepsilon$ upper bound on the local differential privacy (LDP) [17], [18].

To attain LIP, [2] has proposed a watchdog privacy mechanism in which the alphabet of $X$, denoted by $\mathcal{X}$, is bi-partitioned into subsets of low-risk $\mathcal{X}_L = \{x \in \mathcal{X} : \max_i |i(s, x)| \leq \varepsilon \}$ and high-risk, $\mathcal{X}_H = \mathcal{X} \setminus \mathcal{X}_L$ symbols. Then, the low-risk subset is published without alteration and only high-risk symbols are perturbed via a randomization $r_{Y|X}(y|x)$. It has been proved in [3] that any $\alpha$-invariant $r_{Y|X}(y|x)$, e.g., merging all symbols in $\mathcal{X}_H$, minimizes the privacy leakage in $\mathcal{X}_H$. Using $\alpha$-invariant randomization to achieve high level privacy protection could result in low utility.

This paper proposes a method to enhance the utility based on the finer-grained properties of the log-lift. From the intuition behind (1), one can see that a large lift value means that observing $x$ increases the prior belief about the associated sensitive feature $s$, $(\ell(s, x) > 1 \Rightarrow P_{S|X}(s, x) > P_S(s))$. In contrast, a lift value less than one means releasing $x$ decreases the posterior belief. Consequently, both large and small lift values are measures of higher leakage about sensitive features.

To see this clearly, we generalize LIP measures and define the following quantities:

$$ \nu(x) = \min_s i(s, x), \quad \xi(x) = \max_s i(s, x). \quad (2) $$

The existing literature has tried to minimize both $|\nu(x)|$ and $\xi(x)$ or restrict them below a privacy budget. The privacy algorithms in previous works apply the same bound for $|\nu(x)|$ and $\xi(x)$. We call this scenario symmetric local information privacy (SLIP). However, typically, the range of values for $\nu(x)$ and $\xi(x)$ are very different. Fig. 1 shows the histogram
Fig. 1: Histogram of $\nu(x) = \min_i i(s, x)$ and $\xi(x) = \max_i i(s, x)$ for $10^4$ randomly generated distributions with $|X| = 30$, $|S| = 20$. of $\nu(x)$ and $\xi(x)$ for $10^4$ randomly generated distributions with the alphabet size of $|X| = 30$ and $|S| = 20$. We observe that the range of $\nu(x)$ [-15.5, -0.5] is much larger than the range of $\xi(x)$, $[0.3, 1.5]$. Moreover, Fig. 1 shows larger probability values for $\xi(x)$ than $\nu(x)$. Similarly, stemming from the non-negativity of mutual information $I(S; X)$, $P_{S,X}$ is typically much smaller for a very negative $\nu(x)$ than for a very positive $\xi(x)$. Therefore, it seems an unnecessary restriction to apply the same bounds to both of these quantities.

In this work, we generalize LIP by designation of different privacy budgets, $\epsilon_l$ and $\epsilon_u$, for restricting $\nu(x)$ and $\xi(x)$, respectively; and we call it asymmetric local information privacy (ALIP). Then, we investigate the privacy-utility trade-off for ALIP by applying it to the watchdog privacy mechanism. We demonstrate that in ALIP, only max-lift affects the bounds on IT average measures including, MI, maximal leakage, $\alpha$-leakage (Arimoto MI), and Sibson MI; and LDP is upper bounded by $\epsilon = \epsilon_u + \epsilon_l$. We show that for a fixed $\epsilon$, by relaxing of $\nu(x)$ in the watchdog mechanism, ALIP ($\epsilon_l > \epsilon_u$) can not only enhance the utility compared to SLIP ($\epsilon_l = \epsilon_u$), but also provide a tighter upper bound $\epsilon_u$ on the aforementioned IT measures.

II. ASYMMETRIC LOCAL INFORMATION PRIVACY AND THE WATCHDOG MECHANISM

Denote useful data by $X$ with alphabet $X$ and confidential features correlated with it by $S$ with alphabet $S$; they are correlated via joint distribution $(S, X) \sim P_{S,X}$. Our goal is to publish a sanitized version of $X$, denoted by $Y$ with alphabet $Y$, to protect the privacy of $S$ and provide appropriate statistical utility for $X$. They form a Markov chain $S \rightarrow X \rightarrow Y$ where $P_{Y|S,X}(y|s, x) = P_{Y|X}(y|x)$ for all $s, x, y$, and $P_{Y|X}(y|x)$ is the privacy mechanism.

A. Asymmetric Local Information Privacy

**Definition 1.** For a given useful data $X$ and private data $S$ where $(S, X) \sim P_{S,X}$, the privacy mechanism $P_{Y|X}$ satisfies $(\epsilon_l, \epsilon_u)$-ALIP for some $\epsilon_l, \epsilon_u \in \mathbb{R}_+$ if $\forall s, y$:

$$-\epsilon_l \leq i(s, y) \leq \epsilon_u.$$  

(3)

If (3) holds, we say $Y$ is $(\epsilon_l, \epsilon_u)$-ALIP private version of $S$.

**Proposition 1.** When $Y$ is $(\epsilon_l, \epsilon_u)$-ALIP private version of $S$, the following properties are held [2]:

1) $P_{Y|S}$ is $(\epsilon_l + \epsilon_u)$-locally differential private, i.e.

$$\sup_{y, s, s'} \frac{P_{Y|S}(y|s)}{P_{Y|S}(y|s')} \leq e^{\epsilon_l + \epsilon_u}. \quad (4)$$

2) The $\alpha$-lift, mutual information $I(S; Y)$, and maximal leakage between $S$ and $Y$, are upper bounded by $\epsilon_u$.

3) The Sibson MI $I_S^S(S; Y)$ and Arimoto MI $I_A^S(S; Y)$ are upper bounded by $\frac{\alpha}{\alpha - 1} \epsilon_u$.

See Appendices A and B for the proof, which follows the proof of [2, Proposition 1].

Proposition 1-1 means that if $\epsilon = \epsilon_l + \epsilon_u$, then $\epsilon$-LDP is achieved. In other words, LIP methods could be applied to attain LDP. Here, for a fixed $\epsilon$, different values of $\epsilon_u$ and $\epsilon_l$ can be considered to provide different ALIP scenarios, and SLIP ($\epsilon_l = \epsilon_u$) is just one special case. We will show in Section III that for a fixed $\epsilon$, ALIP enhances utility compared to SLIP when $\epsilon_l > \epsilon_u$. This is an interesting property where we can enhance utility for a fixed LDP constraint and at the same time, we can decrease the guessing ability of an adversary by enforcing a more strict bound on $\xi(x)$. Propositions 1-2 and 1-3 show that $\alpha$-lift, mutual information and other mentioned IT measures are upper bounded by $\epsilon_u$. When $\epsilon_l > \epsilon_u$, this means that ALIP can not only improve utility, but also provide a tighter upper bound on other IT measures than SLIP. It should be noted that the watchdog-based utility enhancements in [3] and [19] applied equal bounds on max- and min-lift. [3] relaxed privacy constraints, i.e., allowing some probability of breaching the bounds on lifts; [19] required the search of a locally optimal subset partition of $X_H$. However, we generalize the definition of LIP to match the framework with asymmetric property of the log-lift.

B. Application of ALIP to the Watchdog Mechanism

The watchdog privacy mechanism has been proposed to achieve LIP in [2]. Here, we apply ALIP to it and define the asymmetric privacy watchdog.

**Definition 2.** Asymmetric watchdog privacy mechanism: For a given $(X, S) \sim P_{S,X}$ and $\epsilon_l, \epsilon_u \in \mathbb{R}_+$, the watchdog mechanism bi-partitions $X$ into subsets of low-risk and high-risk symbols $X_L$ and $X_H$, respectively, as follows:

$$X_L \triangleq \{ x \in X : -\epsilon_l \leq i(s, x) \leq \epsilon_u, \quad \forall s \in S \},$$

$$X_H = X \setminus X_L;$$

where $x \in X_L$ are published without perturbation and $x \in X_H$ are randomized via a randomization $r_Y|X(y|x)$. As a result, the privacy mechanism $P_{Y|X}$ is given by:

$$P_{Y|X}(y|x) = \begin{cases} 1_{x=y} & x, y \in X_L; \\ r_Y|X(y|x) & x, y \in X_H; \\ 0 & \text{otherwise}; \end{cases}$$

(6)

where $1_{x=y}$ is the indicator function and $\sum_{y \in X_H} r_Y|X(y|x) = 1$. Similar to SLIP [3], the randomization $r_Y|X(y|x)$ which minimizes the privacy leakage in $X_H$ is an $X$-invariant randomization $R_Y(y)$ that only depends on $y \in X_H$, which is constant for all $x \in X_H$, and is zero otherwise. An instance of $R_Y(y)$ is uniform...
randomization, \( R_Y(y) = \frac{1}{|\mathcal{Y}|}, y \in \mathcal{Y} \). The other option is complete merging which is applied in this paper where all \( x \in \mathcal{X}_H \) are mapped to only one super symbol \( y^* \in \mathcal{Y} \) where \( R_Y(y^*) = 1 \), and \( R_Y(y) = 0, y \neq y^* \).

**Proposition 2.** For a given \((\varepsilon_u, \varepsilon_l)\) and \(\{\mathcal{X}_L, \mathcal{X}_H\}\), \(X\)-invariant randomization \(R_Y(y)\) minimizes the privacy leakage in \(\mathcal{X}_H\). The minimum achievable log-lift upper bound \(\varepsilon^*_u\) and lower bound \(\varepsilon^*_l\) in \(\mathcal{X}_H\), respectively, are given by:

\[
\varepsilon^*_u = \max_s \max_{x \in \mathcal{X}_H} \frac{P(X_H|s)}{P(X_H)},
\]

\[
\varepsilon^*_l = \min_s \min_{x \in \mathcal{X}_H} \frac{P(X_H|s)}{P(X_H)},
\]

where \(P(X_H|s) = \sum_{x \in \mathcal{X}_H} P_{X|S}(x|s), \) and \(P(X_H) = \sum_{x \in \mathcal{X}_H} P_X(x)\).

The proof is similar to the proof of [3, Corollary 2], however, for the sake of completeness it is given in Appendix C.

### C. Utility Measure

To measure utility, we use the normalized mutual information (NMI). Mutual information between \(X\) and \(Y\) in the watchdog mechanism is given by [3]:

\[
I(X; Y) = H(X) + \sum_{x \in \mathcal{X}_H} P_X(x) \log \frac{P_X(x)}{P_X(X_H)}.
\]

Then, the NMI will be: \(\text{NMI} = \frac{I(X; Y)}{H(X)} \in [0, 1]\).

#### III. Numerical Results

In this section, we investigate the properties of ALIP numerically. All results in Sections III-A and III-B have been derived from \(10^4\) randomly generated distributions \(P_{S,X}\) under the asymmetric watchdog mechanism where \(|\mathcal{X}| = 30, |S| = 20\).

##### A. Privacy-Utility Trade-off

In this section, we compare the resulted utility of the asymmetric watchdog mechanism for different values of \(\varepsilon_u\) and \(\varepsilon_l\). Fig. 2 shows the average utility of \(10^4\) randomly generated \(P_{S,X}\) where \(\varepsilon_u \in \{0.6, 0.8, 1\}\) and \(\varepsilon_l \in \{0.4, 0.5, 0.6, \ldots, 6\}\). For each \(\varepsilon_u\), we increase \(\varepsilon_l\) to demonstrate the privacy-utility trade-off.

When \(\varepsilon_u = 0.6\), the maximum utility value is 0.35, a low value due to a strict condition on \(\xi(x)\). When \(\varepsilon_u = 0.8\), the NMI enhances significantly compared with \(\varepsilon_u = 0.6\), and the maximum utility achieves 0.9. However, when \(\varepsilon_u\) increases to 1, utility enhancement is more modest because, in our experiment, most value of \(\xi(x)\)s range between 0.6 and 0.8. Another observation is that the NMI gets mostly saturated after a certain point and does not enhance when increasing \(\varepsilon_l\) since it is already limited by \(\varepsilon_u\).

##### B. ALIP Privacy-Utility trade-off and LDP

Proposition 1-1) explains the relationship between LDP and ALIP, implying that achieving \((\varepsilon_l, \varepsilon_u)\)-ALIP guarantees \(\varepsilon\)-LDP where \(\varepsilon = \varepsilon_l + \varepsilon_u\). We introduce \(\lambda\) for a fixed value of \(\varepsilon\) to have different ALIP scenarios. Here, \(\varepsilon_l = \lambda\varepsilon\) and \(\varepsilon_u = (1 - \lambda)\varepsilon\) for \(\lambda \in [0, 1]\), and SLIP is given by \(\lambda = 0.5\). When \(\lambda < 0.5\), the ALIP utility is smaller than the SLIP utility due to significantly restricted constraint on the min-lift \((\nu(x) < \frac{2}{5})\), therefore, we ignore such cases. When \(\lambda > 0.5\), ALIP enhances utility compared to SLIP by relaxation of min-lift \((\nu(x) > \frac{2}{5})\).

Figs. 3 and 4 illustrate privacy-utility tradeoffs comparison between ALIP and SLIP for \(\varepsilon = 1.5\) and \(\varepsilon = 2\), respectively. They show the cumulative distribution function (CDF) of the utility and privacy leakage for the \(10^4\) randomly generated distributions \(P_{S,X}\) under asymmetric watchdog mechanism. In comparing ALIP with SLIP, we only have shown the value of \(\lambda\) that results in the best overall utility enhancement in our numerical simulations among \(\lambda \in (0.5, 1]\), which is \(\lambda = 0.65\).

As it is shown in Figs. 3(a) and 4(a), ALIP enhances the utility for both values of \(\varepsilon\). In Fig. 3(a), 11% of ALIP cases achieve \(\text{NMI} \geq 0.04\), and in Fig. 4(a) 30% achieve \(\text{NMI} \geq 0.05\), while these percentages are only 4% and 5% for SLIP. Also, the maximum achieved utilities for ALIP are 0.2 and 0.3 for \(\varepsilon = 1.5\) and \(\varepsilon = 2\), respectively, and for SLIP they are 0.1 and 0.2. When \(\varepsilon = 2\), ALIP results in better utility enhancement than \(\varepsilon = 1.5\) due to a higher total LDP privacy budget.

Figs. 3(b) and 3(c) show the min-lift and max-lift privacy leakage, respectively, for \(\varepsilon = 1.5\). Compared to SLIP, ALIP results in greater min-lift leakage (Fig. 3(b)) and a lower max-lift leakage (Fig. 3(c)) that demonstrate our claim in proposition 1. Privacy leakages for \(\varepsilon = 2\) are shown in Figs. 4(b) and 4(c). Here, we have higher leakage for both SLIP and ALIP due to higher privacy budget, and again ALIP results in higher min-lift and lower max-lift leakage compared to SLIP.

We should note that, although complete merging minimizes privacy leakage in \(\mathcal{X}_H\), there is a chance that after watchdog randomization, the privacy budget in \(\mathcal{X}_H\) is not attained [3], [20]. If the privacy constraints are not satisfied, a simple idea is to move more elements form \(\mathcal{X}_L\) to \(\mathcal{X}_H\) (at the cost of reduced utility).

##### C. Real-world dataset

In this section, we demonstrate log-lift asymmetry and SLIP and ALIP watchdog mechanism on the real-world adult dataset [21], where \(S \in \{\text{marital status}\}, X \in \{\text{occupation}\}, |\mathcal{X}| = 15, |S| = 7, \) and \(\varepsilon \in \{1, 1.5, 2, \ldots, 5\}\).
with symmetric-LIP. The range of \( \nu(x) \) in Fig. 5(a) is \([-12, -0.3]\) with a maximum probability of 0.03, while \( \xi(x) \) has the range of \([0.096, 1.5]\) with a maximum probability of 0.08; thus, they demonstrate asymmetry in their values and probabilities. Fig. 5(b) shows utility comparison for SLIP and ALIP (\( \lambda = 0.55 \)), where ALIP enhances utility when \( \varepsilon \in \{1.5, 2\} \). Figs. 5(c) and 5(d) illustrate min-lift and max-lift privacy leakages. Both ALIP and SLIP satisfy privacy constraints for all values of \( \varepsilon \). Fig. 5(c) shows that ALIP results in higher min-lift leakage compared to SLIP when \( \varepsilon \in \{1.5, 2\} \), while Fig. 5(d) shows it achieves the same max-lift leakage as SLIP for all values of \( \varepsilon \).

### IV. Conclusion

In this paper, we proposed a generalized definition of LIP and applied it to the watchdog mechanism where different values of privacy budgets are allocated to the maximum and minimum of log-lift. We called it asymmetric local information privacy. Then we investigated the privacy-utility trade-off in this mechanism. It is demonstrated that for a fixed privacy budget on LDP, ALIP can enhance utility when we have relaxation on minimum lift values while restricting maximum lift values. Moreover, since other privacy measures such as MI, Sibson MI, \( \alpha \)-lift, \( \alpha \)-leakage are upper bounded by the maximum lift, ALIP tightly bounds these measures compared with symmetric-LIP.

For future works, it is worth considering other privacy mechanisms rather than the watchdog mechanism by investigating the effects of ALIP on the privacy-utility trade-off for them. Estimation of the distribution of log-lift is also an open problem that could be considered in connection with ALIP. Combination of other relaxation methods such as \( (\varepsilon, \delta) \) with ALIP can also be considered.

### Appendix

**A. Definitions**

**Definition 3.** For discrete \( (S, Y) \sim P_{S,Y} \) and \( \alpha \in (1, \infty) \), the Arimoto MI which is equivalent to the \( \alpha \)-leakage [16], is given by

\[
I^A_\alpha(S; Y) = \frac{\alpha}{\alpha - 1} \log \frac{\mathbb{E}_Y \left[ \left\| P_{S|Y} \right\|_\alpha \right]}{\| P_S \|_\alpha}. \tag{10}
\]

**Definition 4.** For discrete \( (S, Y) \sim P_{S,Y} \), Sibson’s MI is given by

\[
I^S_\alpha(S; Y) = \frac{\alpha}{\alpha - 1} \log \sum_{y \in Y} \left( \sum_{s \in S} P_S(s) P_{Y|S}(y|s) \right)^{\frac{1}{\alpha}}. \tag{11}
\]

**Definition 5.** For discrete \( (S, Y) \sim P_{S,Y} \), and \( \alpha \in (1, \infty) \), the \( \alpha \)-lift [14], is given by

\[
\ell_\alpha(y) = \left( \sum_{s \in S} P_S(s) \left( \frac{P_{S,Y}(s, y)}{P_S(s) P_Y(y)} \right) \right)^{1/\alpha}, \quad \forall y \in Y. \tag{12}
\]
For \( \alpha = 1 \), Sibson and Arimoto MI reduce to Shannon’s MI. For \( \alpha = \infty \), the Arimoto MI will be

\[
I_{\infty}^A(S; Y) = \log \sum_{s \in S} P_Y(s) P_Y(s|Y).
\]

(13)

\( \alpha \)-lift reduces to maximum of the lift \( \ell_{\infty}(s) = \max_{x \in \mathcal{S}} \ell(s, y) \), and the Sibson MI is given by

\[
I_{\infty}^S(S; Y) = \log \mathbb{E}_{Y} [\max_{s \in \mathcal{S}} \ell(s, Y)],
\]

which is equivalent to the maximal leakage.

B. Proof of Proposition 1

Proposition 1-1: For any \( s, s' \in \mathcal{S} \), assume \( P_{S,Y}(s, y) > 0 \) and \( P_{S,Y}(s', y) > 0 \), by Definition 1 we have:

\[
\left| \log \frac{P_{Y|S}(y|s)}{P_{Y|S}(y|s')} \right| = \left| \log \frac{P_{Y|S}(y|s)}{P_{S}(y)} - \log \frac{P_{Y|S}(y|s')}{P_{S}(y)} \right| \leq \varepsilon_u + \varepsilon_l.
\]

Proposition 1-2: For mutual information we have:

\[
I(S; Y) = \mathbb{E}_{P_{S,Y}[i(S, Y)]} \leq \sum_{s \in \mathcal{S}} P_{S}(s) I(s, Y).
\]

For \( \alpha \)-lift, using Jensen inequality and Definition 1 we have:

\[
1 \leq \ell_{\alpha}(y) \leq e^{\varepsilon_u} \alpha.
\]

C. Proof of Proposition 2

We follow the steps in proof of [3, Corollary 2]. Let \( s_u \in \text{argmax} P_{X|S}(X|s) \) and \( s_t \in \text{argmin} P_{X|S}(X|s_t) \). Proposition 2 is proven by contradiction. Assume there exists another \( r_{Y|X}(y|x) \) that attains lifts strictly smaller than \( e^{-\varepsilon_l} \) and \( e^{\varepsilon_u} \).

Then both:

\[
\frac{\sum_{x \in X_H} r_{Y|X}(y|x) P_{X|S}(x|s)}{\sum_{x \in X_H} r_{Y|X}(y|x) P_X(x)} < \frac{P(X_H|s_u)}{P(X_H)} := \ell(s_u, X_H)
\]

(15)

\[
\frac{\sum_{x \in X_H} r_{Y|X}(y|x) P_{X|S}(x|s)}{\sum_{x \in X_H} r_{Y|X}(y|x) P_X(x)} > \frac{P(X_H|s_t)}{P(X_H)} := \ell(s_t, X_H)
\]

(16)

hold for all \( y \in X_H \) and \( s \in \mathcal{S} \). However, for any \( y \), we have

\[
\sum_{x \in X_H} r_{Y|X}(y|x) P_{X|S}(x|s) - P(X_H|s_u) P_X(x)
\]

\[
\sum_{x \in X_H} r_{Y|X}(y|x) P_{X|S}(x|s) - P(X_H|s_t) P_X(x)
\]

(17)

(18)

(19)

Inequality (18) holds because, for all \( y' \in X_H \) with \( y' \neq y \), (15) holds and therefore

\[
\sum_{x \in X_H} r_{Y|X}(y'|x) (P(X_H|X|s) - P(X_H|s_t) P_X(x)) < 0.
\]

For \( s = s_u \), (19) will be 0, i.e., (15) does not hold, which is a contradiction. To show the contradiction in (16), consider the numerator of (17) and replace \( s_u \) with \( s_t \). We have

\[
\sum_{x \in X_H} r_{Y|X}(y|x) (P(X_H) - P(X_H|s_t) P_X(x))
\]

\[
= \sum_{x \in X_H} \left( 1 - \sum_{x_H|y'} \sum_{y|x} r_{Y|X}(y|x) (P(X_H|X|s) - P(X_H|s_t) P_X(x)) \right)
\]

\[
= \sum_{x \in X_H} \left( P(X_H) - P(X_H|s_t) P_X(x) \right)
\]

which contradicts (16) for \( s = s_t \). Therefore, Proposition 2 holds.
REFERENCES

[1] F. du Pin Calmon and N. Fawaz, “Privacy against statistical inference,” in 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton). IEEE, 2012, pp. 1401–1408.

[2] H. Hou, S. Asoodeh, and F. d. P. Calmon, “Information-theoretic privacy watchdogs,” in Proc. IEEE Int. Symp. Inf. Theory, Paris, France, 2019, pp. 552–556.

[3] P. Sadeghi, N. Ding, and T. Rakotoariveloh, “On properties and optimization of information-theoretic privacy watchdog,” in Proc. IEEE Inf. Theory Workshop, 2020.

[4] N. Ding, Y. Liu, and F. Farokhi, “A linear reduction method for local differential privacy and log-lift,” in 2021 IEEE International Symposium on Information Theory (ISIT), 2021, pp. 551–556.

[5] B. Jiang, M. Li, and R. Tandon, “Context-aware data aggregation with localized information privacy,” in 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1–9.

[6] ——, “Local information privacy with bounded prior,” in 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1–7.

[7] M. Seif, R. Tandon, and M. Li, “Context aware Laplacian mechanism for local information privacy,” in 2019 IEEE Information Theory Workshop (ITW), 2019, pp. 1–5.

[8] B. Jiang, M. Li, and R. Tandon, “Local information privacy and its application to privacy-preserving data aggregation,” IEEE Transactions on Dependable and Secure Computing, pp. 1–1, 2020.

[9] B. Jiang, M. Seif, R. Tandon, and M. Li, “Context-aware local information privacy,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3694–3708, 2021.

[10] B. Razeghi, F. Calmon, D. Gunduz, and S. Voloshynovskiy, “On perfect obfuscation: Local information geometry analysis,” arXiv preprint arXiv:2009.04157, 2020.

[11] B. Rassouli and D. Gunduz, “Optimal utility-privacy trade-off with total variation distance as a privacy measure,” IEEE Transactions on Information Forensics and Security, 2019.

[12] A. Makhdoumi, S. Salamatian, N. Fawaz, and M. Médard, “From the information bottleneck to the privacy funnel,” in 2014 IEEE Information Theory Workshop (ITW 2014), Nov 2014, pp. 501–505.

[13] I. Issa, S. Kamath, and A. B. Wagner, “An operational measure of information leakage,” in 2016 Ann. Conf. Inf. Sci. Syst., Princeton, NJ, 2016, pp. 234–239.

[14] N. Ding, M. A. Zarrabian, and P. Sadeghi, “α-information-theoretic privacy watchdog and optimal privatization scheme,” in Proc. IEEE Int. Symp. Inf. Theory, 2021, pp. 2584–2589.

[15] S. Verdú, “α-mutual information,” in Proc. Information Theory and Applications Workshop (ITA), San Diego, CA, 2015, pp. 1–6.

[16] J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, “A tunable measure for information leakage,” in IEEE International Symposium on Information Theory (ISIT). IEEE, 2018, pp. 701–705.

[17] S. P. Kasiviswanathan, H. K. Lee, K. Nissim, S. Raskhodnikova, and A. Smith, “What can we learn privately?” SIAM Journal on Computing, vol. 40, no. 3, pp. 793–826, 2011.

[18] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, “Local privacy and statistical minimax rates,” in Proc. IEEE 54th Annu. Symp. Found. Comput. Sci., 2013, pp. 429–438.

[19] M. A. Zarrabian, N. Ding, P. Sadeghi, and T. Rakotoariveloh, “Enhancing utility in the watchdog privacy mechanism,” 2022. [Online]. Available: https://arxiv.org/abs/2110.04724

[20] H. Hsu, S. Asoodeh, and F. Calmon, “Obfuscation via information density estimation,” in International Conference on Artificial Intelligence and Statistics. PMLR, 2020, pp. 906–917.