Bounds for Privacy-Utility Trade-off with Per-letter Privacy Constraints and Non-zero Leakage

Amirreza Zamani, Tobias J. Oechtering, Mikael Skoglund

Division of Information Science and Engineering, KTH Royal Institute of Technology
Email: amizam@kth.se, oech@kth.se, skoglund@kth.se

Abstract—An information theoretic privacy mechanism design problem for two scenarios is studied where the private data is either hidden or observable. In each scenario, privacy leakage constraints are considered using two different measures. In these scenarios the private data is hidden or observable. In the first scenario, an agent observes useful data $Y$ that is correlated with private data $X$, and wishes to disclose the useful information to a user. A privacy mechanism is designed to generate disclosed data $U$ which maximizes the revealed information about $Y$ while satisfying a per-letter privacy constraint. In the second scenario, the agent has additional access to the private data. First, the Functional Representation Lemma and Strong Functional Representation Lemma are extended by relaxing the independence condition to find a lower bound considering the second scenario. Next, lower bounds as well as upper bounds on privacy-utility trade-off are derived for both scenarios. In particular, for the case where $X$ is deterministic function of $Y$, we show that our upper and lower bounds are asymptotically optimal considering the first scenario.

I. INTRODUCTION

The privacy mechanism design problem is recently receiving increased attention in information theory [1]–[21]. Specifically, in [1], the concept of a privacy funnel is introduced, where the privacy utility trade-off has been studied considering a distortion measure for utility and the log-loss as privacy measure. In [2], the concept of maximal leakage has been introduced and some bounds on the privacy utility trade-off have been derived. Fundamental limits of the privacy utility trade-off measuring the leakage using estimation-theoretic guarantees are studied in [3]. A related secure source coding problem is studied in [4].

The problem of privacy-utility trade-off considering mutual information both as measure of utility and privacy is studied in [5]. Under the perfect privacy assumption it is shown that the privacy mechanism design problem can be reduced to a linear program. Moreover, it has been shown that information can be only revealed if the kernel (leakage matrix) between useful data and private data is not invertible. In [6], we generalize [5] by relaxing the perfect privacy assumption allowing some small bounded leakage. More specifically, we design privacy mechanisms with a per-letter privacy criterion considering an invertible kernel where a small leakage is allowed. We generalized this result to a non-invertible leakage matrix in [7].

In this paper, random variable (RV) $Y$ denotes the useful data and is correlated with the private data denoted by RV $X$. Furthermore, RV $U$ describes the disclosed data. Two scenarios are considered in this work, where in both scenarios, an agent wants to disclose the useful information to a user as shown in Fig. 1. In the first scenario, the agent observes $Y$ and has not directly access to $X$, i.e., the private data is hidden. The goal is to design $U$ based on $Y$ that reveals as much information as possible about $Y$ and satisfies a privacy criterion. In the second scenario, the agent has access to both $X$ and $Y$ and can design $U$ based on $(X, Y)$ to release as much information as possible about $Y$ while satisfying the leakage constraint. In both scenarios we consider two different per-letter privacy criterion.

In [8], by using the Functional Representation Lemma bounds on privacy-utility trade-off for the two scenarios are derived. These results are derived under the perfect secrecy assumption, i.e., no leakages are allowed. In [9], we generalize the privacy problems considered in [8] by relaxing the perfect privacy constraint and allowing some leakages. Furthermore, in the special case of perfect privacy we found a new upper bound for the perfect privacy function by using the excess functional information introduced in [22]. It has been shown that this new bound generalizes the bound in [8].

In [9], mutual information is used for measuring the privacy leakage, however in the present work, for each scenario we use two different per-letter privacy constraints. As argued in [7], it is more desirable to protect the private data individually and not on average. By using an average constraint, a data point can exist which leaks more than the average threshold.

In this work, we first derive similar lemmas as [9, Lemma 3] and [9, Lemma 4] considering per-letter privacy constraint
rather than bounded mutual information. Using these lemmas we find a lower bound for the privacy-utility trade-off in the second scenario with first per letter leakage constraint. Furthermore, we provide bounds for three other problems and study a special case where $X$ is a deterministic function of $Y$. In this case, we show that the obtained upper and lower bounds in the first scenario are asymptotically optimal. Finally, we evaluate the bounds in a numerical example. In the extended version [23], complete proofs of this work and more discussions on the new bounds are provided.

II. SYSTEM MODEL AND PROBLEM FORMULATION

Let $P_{XY}$ denote the joint distribution of discrete random variables $X$ and $Y$ defined on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$ with $|\mathcal{X}| < |\mathcal{Y}|$. We represent $P_{XY}$ by a matrix defined on $\mathbb{R}^{|\mathcal{X}| \times |\mathcal{Y}|}$ and marginal distributions of $X$ and $Y$ by vectors $P_X$ and $P_Y$ defined on $\mathbb{R}^{|\mathcal{X}|}$ and $\mathbb{R}^{|\mathcal{Y}|}$ given by the row and column sums of $P_{XY}$. We assume that each element in vectors $P_X$ and $P_Y$ is non-zero. Furthermore, we represent the leakage matrix $P_{XY}$ by a matrix defined on $\mathbb{R}^{|\mathcal{X}| \times |\mathcal{Y}|}$, which is assumed to be of full rank. Furthermore, for given $u \in \mathcal{U}$, $P_{X,u}, (\cdot,u)$ and $P_{X|u}(\cdot|u)$ defined on $\mathbb{R}^{|\mathcal{X}|}$ are distribution vectors with elements $P_{X,u}(x,u)$ and $P_{X|u}(x|u)$ for all $x \in \mathcal{X}$ and $u \in \mathcal{U}$. The relation between $U$ and $Y$ is described by the kernel $P_{UY}$ defined on $\mathbb{R}^{|\mathcal{U}| \times |\mathcal{Y}|}$, furthermore, the relation between $U$ and the pair $(Y,X)$ is described by the kernel $P_{UY|X}$ defined on $\mathbb{R}^{|\mathcal{U}| \times |\mathcal{Y}| \times |\mathcal{X}|}$.

The privacy mechanism design problems for the two scenarios can be stated as follows

\begin{align}
\tag{1} g^1_\epsilon(P_{XY}) &= \sup_{P_{U|Y: X-Y-U}} \quad I(Y;U), \\
\tag{2} h^1_\epsilon(P_{XY}) &= \sup_{P_{U|Y: |U}; P_X, P_{P_U}(u)} \quad I(Y;U), \\
\tag{3} g^2_\epsilon(P_{XY}) &= \sup_{P_{U|Y: X-Y-U}} \quad I(Y;U), \\
\tag{4} h^2_\epsilon(P_{XY}) &= \sup_{P_{U|Y: |U}; P_X, P_{P_U}(u)} \quad I(Y;U),
\end{align}

where $d(P,Q)$ corresponds to the total variation distance between two distributions $P$ and $Q$, i.e., $d(P,Q) = \sum_x |P(x) - Q(x)|$. The functions $h^1_{\epsilon}(P_{XY})$ and $h^2_{\epsilon}(P_{XY})$ are used when the privacy mechanism has access to both the private data and the useful data. The functions $g^1_{\epsilon}(P_{XY})$ and $g^2_{\epsilon}(P_{XY})$ are used when the privacy mechanism has access to the useful data only. In this work, the privacy constraints used in (1) and (3), i.e., $d(P_{X,u}(\cdot,u), P_X P_U(u)) \leq \epsilon$, $\forall u$, and $d(P_{X|u}(\cdot|u), P_X) \leq \epsilon$, $\forall u$, are called the strong privacy criterion 1 and the strong privacy criterion 2. We refer to them as strong since they are per-letter privacy constraints, i.e., they must hold for every $u \in \mathcal{U}$. The difference between the two privacy constraints is the weight $P_U(u)$, which we later show enables us to use extended versions of the Functional Representation Lemma and Strong Functional Representation Lemma to find lower bounds considering the second scenario.

Remark 1. The leakage constraint $d(P_{X|U}(\cdot|u), P_X) \leq \epsilon$, $\forall u$ has been used in [7], where we called it the strong $\ell_1$-privacy criterion.

Remark 2. For $\epsilon = 0$, both (1) and (3) lead to the perfect privacy problem studied in [5]. It has been shown that for a non-invertible leakage matrix $P_{X|Y}, g_0(P_{XY})$ can be obtained by a linear program [5].

Remark 3. For $\epsilon = 0$, both (2) and (4) lead to the secret-dependent perfect privacy function $h_0(P_{XY})$ studied in [8], where upper and lower bounds on $h_0(P_{XY})$ have been derived. In [9], we have strengthened these bounds.

Remark 4. The privacy problem defined in (3) has been studied in [7], where we provide a lower bound on $d^2(P_{XY})$ using information geometry concepts. Furthermore, we have shown that, without loss of optimality, it is sufficient to assume $|U| \leq |\mathcal{Y}|$ so that it is ensured that the supremum can be achieved.

Intuitively, for small $\epsilon$, both privacy constraints mean that $X$ and $U$ are almost independent. As we discussed in [7], closeness of $P_{X|U}(\cdot|u)$ and $P_X$ allows us to approximate $g^1_{\epsilon}(P_{XY})$ and find a lower bound. Furthermore, in this work we show that by using similar steps as [7], we can approximate $g^2_{\epsilon}(P_{XY})$ using closeness of $P_{X|U}(\cdot,u)$ and $P_X P_U(u)$. This provides us a lower bound for $g^1_{\epsilon}(P_{XY})$. Next, we study some properties of the strong privacy criterion 1 and the strong privacy criterion 2. To this end recall that the linkage inequality is the property that if $L$ measures the privacy leakage between two random variables and the Markov chain $X - Y - U$ holds then we have $L(X;U) \leq L(Y;U)$. Since the strong privacy criterion 1 and the strong privacy criterion 2 are per-letter constraints we define $L^1(X;U = u) \triangleq \|P_{X|U}(\cdot|u) - P_X\|_1$, $L^1(Y;U = u) \triangleq \|P_{Y|U}(\cdot|u) - P_Y\|_1$, $L^2(X;U = u) \triangleq \|P_{X|U}(\cdot,u) - P_X P_U(u)\|_1$, $L^2(Y;U = u) \triangleq \|P_{Y|U}(\cdot,u) - P_Y P_U(u)\|_1$.

Proposition 1. The strong privacy criterion 1 and the strong privacy criterion 2 satisfy the linkage inequality. Thus, for each $u \in \mathcal{U}$ we have $L^1(X;U = u) \leq L^1(Y;U = u)$ and $L^2(X;U = u) \leq L^2(Y;U = u)$.

Proof. The proof is provided in Appendix A.\hfill $\Box$

A discussion on the benefits of the linkage inequality is provided in [23, page 2]. Next, given a leakage measure $L$ and let the Markov chain $X - Y - U$ hold, if we have $L(X;U) \leq L(X;Y)$, then we say that the post processing inequality holds. In this work we use $L^1(X;U) = \sum_u P_U(u) L^1(X;U = u)$, $L^2(X;U) = \sum_u L^2(X;U = u)$ and $L^1(Y;U) = \sum_u P_U(u) L^1(Y;U = u)$, $L^2(Y;U) = \sum_u L^2(Y;U = u)$.

Proposition 2. The average of the strong privacy criterion 1 and 2 with weights $1$ and $P_U(u)$, respectively, satisfy the post processing inequality, i.e., we have $L^1(X;U) \leq L^1(Y;U)$ and $L^2(X;U) \leq L^2(Y;U)$.
Proof. The proof follows similar lines as [14, Theorem 3] which is based on the convexity of the \( \ell_1 \)-norm. \(\square\)

**Proposition 3.** The strong privacy criterion 1 and 2 result in bounded inference threat that is modeled in [17].

**Proof.** The strong privacy criterion 1 and 2 lead to a bound on average constraint \( \sum_u P_U(u) \left| P_{X|U=u} - P_X \right|_1 = 2TV(X;U) \leq \epsilon \), where \( TV(\cdot,\cdot) \) corresponds to the total variation. Thus, using [14, Theorem 4], we obtain that inference threats are bounded. \(\square\)

Another property of \( \ell_1 \)-distance is the relation between the \( \ell_1 \)-norm and probability of error in a hypothesis test, which is discussed in [23, page 3]. Finally, if we use \( \ell_1 \)-distance as privacy leakage measure, after approximating \( g_1^2(P_{XY}) \) and \( g_2^2(P_{XY}) \), we face linear program problems in the end, which are much easier to handle.

### III. MAIN RESULTS

In this section, we first obtain a lower bound on \( h_1^1(P_{XY}) \) using Lemma 2 and Lemma 3 provided in Appendix B. Both lemmas are similar to [9, Lemma 3] and [9, Lemma 4], where we replace mutual information, i.e., \( I(U;X) = \epsilon \), with a per-letter constraint, i.e., the strong privacy criterion 1. In the remaining part of this work \( d(\cdot,\cdot) \) corresponds to the total variation distance, i.e., \( d(P,Q) = \sum_x |P(x) - Q(x)|. \)

**Proposition 4.** For any \( 0 \leq \epsilon < \sqrt{2I(X;Y)} \) and pair of RVs \( (X,Y) \) distributed according to \( P_{XY} \) supported on alphabets \( X \) and \( Y \) we have

\[
\begin{align*}
    h_1^1(P_{XY}) & \geq \max \{ L_{h_1^1}(\epsilon), L_{h_2^1}(\epsilon) \}, \\
    L_{h_1^1}(\epsilon) &= H(Y|X) - H(X|Y) + \frac{\epsilon^2}{2}, \\
    L_{h_2^1}(\epsilon) &= H(Y|X) - \alpha H(X|Y) + \frac{\epsilon^2}{2} - (1 - \alpha) (\log(I(X;Y) + 1) + 4),
\end{align*}
\]

where \( \alpha = \frac{\epsilon^2}{2I(X;Y)} \).

**Proof.** The proof is provided in [23, Proposition 4]. \(\square\)

In [23, Section III-A], we provide a lower bound on \( g_1^1(P_{XY}) \) following the same approach as in [7]. For more details see [23, Section III-A]. In the following result, \( L_{h_1^1}(\epsilon) \) corresponds to the lower bound for \( g_1^1(P_{XY}) \), which is derived in [23, Lemma 4].

**Theorem 1.** For sufficiently small \( \epsilon \geq 0 \) and any pair of RVs \( (X,Y) \) distributed according to \( P_{XY} \) supported on alphabets \( X \) and \( Y \) we have

\[
L_{g_1^1}(\epsilon) \leq g_1^1(P_{XY}),
\]

and for any \( \epsilon \geq 0 \) we obtain

\[
\begin{align*}
    g_1^1(P_{XY}) & \leq \frac{\epsilon|Y||X|}{\min P_X} + H(Y|X) = U_{g_1}(\epsilon), \\
    g_1^1(P_{XY}) & \leq h_1^1(P_{XY}).
\end{align*}
\]

Furthermore, for any \( 0 \leq \epsilon \leq \sqrt{2I(X;Y)} \) we have

\[
\max \{ L_{h_1^1}(\epsilon), L_{h_2^1}(\epsilon) \} \leq h_1^1(P_{XY}),
\]

where \( L_{h_1^1}(\epsilon) \) and \( L_{h_2^1}(\epsilon) \) are defined in Proposition 4.

**Proof.** Lower bounds on \( g_1^1(P_{XY}) \) and \( h_1^1(P_{XY}) \) are derived in [23, Lemma 4] and Proposition 4, respectively. Furthermore, inequality \( g_1^1(P_{XY}) \leq h_1^1(P_{XY}) \) holds since \( h_1^1(P_{XY}) \) has fewer constraints. To prove the upper bound on \( g_1^1(P_{XY}) \), i.e., \( U_{g_1}(\epsilon) \), let \( U \) satisfy \( X - Y - U \) and the strong privacy criterion 1, then we have

\[
\begin{align*}
    I(U;Y) &= I(X;U) + H(Y|X) - I(X;U|Y) - H(Y|X,U) \\
    &\leq I(X;U) + H(Y|X) \\
    &= \sum_u P_U(u) D(P_{X|U=u},P_X) + H(Y|X) \\
    &\leq \sum_u P_U(u) \left( \frac{d(P_{X|U=u},P_X)^2}{\min P_X} \right) + H(Y|X) \\
    &\leq \sum_u P_U(u) \left( \frac{d(P_{X|U=u},P_X)^2}{\min P_X} \right) |X| + H(Y|X) \\
    &\leq \frac{\epsilon|Y||X|}{\min P_X} + H(Y|X),
\end{align*}
\]

where (a) follows by the reverse Pinsker inequality [24, inequality (23)] and (b) holds since \( d(P_{X|U=u},P_X) = \sum_i |P_{X|U}(x_i|u) - P_X(x_i)| \leq |X| \). Moreover, (c) holds since by suing [23, Proposition 5], we can assume \( |U| \leq |Y| \) without loss of optimality. In other words, (c) holds since by [23, Proposition 5] we have

\[
g_1^1(P_{XY}) = \max_{P_{U|Y} : |X-Y-U|} I(Y;U). \tag{6}
\]

In the next section we provide bounds for \( g_2^2(P_{XY}) \) and \( h_2^2(P_{XY}) \).

### A. Lower and Upper bounds for \( g_2^2(P_{XY}) \) and \( h_2^2(P_{XY}) \)

As we mentioned earlier, we have provided an approximate solution for \( g_2^2(P_{XY}) \) using local approximation of \( H(Y|U) \) for sufficiently small \( \epsilon \) in [7]. Moreover, in [7, Proposition 8] we specified permissible leakages. By using [7, Proposition 2], we can write

\[
\begin{align*}
    g_2^2(P_{XY}) &= \max_{d(P_{X|U}(\cdot|u),P_X) \leq \epsilon, \forall u} I(Y;U). \tag{7}
\end{align*}
\]

In the next lemma we find a lower bound for \( g_2^2(P_{XY}) \), where we use the approximate problem for (3).

**Lemma 1.** Let the kernel \( P_{U|Y} \) achieve the optimum solution in [7, Theorem 2]. Thus, \( I(U^*;Y) \) achieved by this kernel is a lower bound for \( g_2^2(P_{XY}) \). In other words, we have

\[
g_2^2(P_{XY}) \geq I(U^*;Y) = L_{g_2^1}(\epsilon).
\]

\(\square\)
Proof. The proof follows since the kernel $P_{U|Y}$ that achieves the approximate solution satisfies the constraints in (3). □

Next we provide upper bounds for $g_2^2(P_{XY})$. To do so, we first bound the approximation error in [7, Theorem 2]. Let the approximation error be the distance between $H(Y|U)$ and the approximation derived in [7, Theorem 2].

**Proposition 5.** For all $0 < \epsilon < \frac{1}{2} \epsilon_2$, we have

$$|\text{Approximation error}| < \frac{3}{4},$$

Furthermore, for all $0 < \epsilon < \frac{1}{2} \epsilon_2$, the upper bound can be strengthened as follows

$$|\text{Approximation error}| < \frac{1}{2(2\sqrt{|X|} - 1)^2} + \frac{1}{4|X|},$$

where $\epsilon_2$ is defined in [23, Proposition 8].

**Proof.** The proof is provided in [23, Appendix C]. □

As a result we can find an upper bound on $g_2^2(P_{XY})$. To do so let $\text{approx}(g_2^2)$ be the value that the kernel $P_{U|Y}$ in Lemma 1 achieves, i.e., the approximate value in [7, Theorem 2].

**Corollary 1.** For any $0 \leq \epsilon < \frac{1}{2} \epsilon_2$ we have

$$g_2^2(P_{XY}) \leq \text{approx}(g_2^2) + \frac{3}{4} = U_{g_2}(\epsilon),$$

furthermore, for any $0 \leq \epsilon < \frac{1}{2} \epsilon_2$ the upper bound can be strengthened as

$$g_2^2(P_{XY}) \leq \text{approx}(g_2^2) + \frac{1}{2(2\sqrt{|X|} - 1)^2} + \frac{1}{4|X|} = U_{g_2}(\epsilon).$$

In the next theorem, we summarize the bounds for $g_2^2(P_{XY})$ and $h_2^2(P_{XY})$, furthermore, a new upper bound on $h_2^2(P_{XY})$ is derived.

**Theorem 2.** For any $0 \leq \epsilon < \frac{1}{2} \epsilon_2$ and pair of RVs $(X, Y)$ distributed according to $P_{XY}$ supported on alphabets $X$ and $Y$ we have

$$L_{g_2}(\epsilon) \leq g_2^2(P_{XY}) \leq U_{g_2}(\epsilon),$$

and for any $0 \leq \epsilon < \frac{1}{2} \epsilon_2$ we get

$$L_{g_2}(\epsilon) \leq g_2^2(P_{XY}) \leq U_{g_2}(\epsilon),$$

furthermore, for any $0 \leq \epsilon$$

$$g_2^2(P_{XY}) \leq h_2^2(P_{XY}) \leq \frac{\epsilon^2}{\min P_X} + H(Y|X) = U_{h_2}(\epsilon).$$

**Proof.** It suffices to show that the upper bound on $h_2^2(P_{XY})$ holds. To do so, let $U$ satisfy $d(P_{X|U}(\cdot|u), P_X) \leq \epsilon$, then we have

$$I(U; Y) = I(X; U) + H(Y|X) - I(X; U|Y) - H(Y|X, U) \leq I(X; U) + H(Y|X) \leq \epsilon^2 \min P_X + H(Y|X),$$

where (a) follows by the reverse Pinsker inequality. □

In next section, we study the special case where $X$ is a deterministic function of $Y$, i.e., $H(X|Y) = 0$.

**B. Special case: $X$ is a deterministic function of $Y$**

By using (6) and (7) we obtain the next corollary.

**Corollary 2.** For any $0 \leq \epsilon \leq \sqrt{2|I(X; Y)|}$ we have

$$\max\{L_{h_2}(\epsilon), L_{g_2}(\epsilon), U_{h_2}(\epsilon)\} \leq g_2^0(P_{XY}) \leq U_{g_2}(\epsilon).$$

We can see that the bounds in Corollary 2 are asymptotically optimal. The latter follows since in high privacy regimes, i.e., the leakage tends to zero, $U_{h_2}(\epsilon)$ and $L_{h_2}(\epsilon)$ both tend to $H(Y|X)$, which is the optimal solution to $g_0(P_{XY})$ when $X$ is a deterministic function of $Y$, [8, Theorem 6]. Furthermore, by using Theorem 2 and (9) we obtain the next result.

**Corollary 3.** For any $0 \leq \epsilon < \frac{1}{2} \epsilon_2$ we have

$$L_{g_2}(\epsilon) \leq g_2^2(P_{XY}) \leq \min\{L_{g_2}(\epsilon), U_{g_2}(\epsilon)\}.$$
Fig. 2. Comparing the upper bound and lower bound for $g_2^X$. The upper bounds $U_{12}^X(\epsilon)$ and $U_{22}^X(\epsilon)$ are valid for $\epsilon < 0.0171$ and $\epsilon < 0.0121$, respectively. On the other hand, the upper bound $U_{02}^X(\epsilon)$ is valid for all $\epsilon \geq 0$.

Fig. 3. Comparing the upper bound and lower bound for $g_2^X$. $\epsilon > 0$.

Fig. 4. Comparing the upper bound and lower bound for $g_2^X$. The upper bounds $U_{12}^X(\epsilon)$ and $U_{22}^X(\epsilon)$ are valid for $\epsilon < 0.0997$ and $\epsilon < 0.0705$, respectively. However, the upper bound $U_{02}^X(\epsilon)$ is valid for all $\epsilon \geq 0$.

Fig. 5. Comparing the upper bound and lower bound for $g_2^X$. $\epsilon > 0$.

**APPENDIX A**

For each $u \in \mathcal{U}$ we have

$$L^1(X; U = u) = \|P_{X|U=u}(\cdot|u) - P_X\|_1$$

$$= \|P_{X|Y}(P_{Y|U=u}(\cdot|u) - P_Y)\|_1$$

$$= \sum_y \left| \sum_x P_{X|Y}(x|y)(P_{Y|U=u}(y) - P_Y(y)) \right|$$

$$\leq \sum_y \sum_x P_{X|Y}(x|y)|P_{Y|U=u}(y) - P_Y(y)|$$

$$= \sum_y \sum_x P_{X|Y}(x|y)|P_{Y|U=u}(y) - P_Y(y)|$$

$$= \|P_{Y|U=u} - P_Y\|_1 = L^1(Y; U = u),$$

where (a) follows from the triangle inequality. Furthermore, we can multiply all the above expressions by the term $P_U(u)$ so that we obtain $L^2(X; U = u) \leq L^2(Y; U = u)$.

**APPENDIX B**

Lemma 2. For any $0 \leq \epsilon < \sqrt{2I(X; Y)}$ and any pair of RVs $(X, Y)$, there exists a RV $U$ supported on $\mathcal{U}$ such that $X$ and $U$ satisfy the strong privacy criterion 1, i.e., we have

$$d(P_{X,U}(\cdot, u), P_X P_U(u)) \leq \epsilon, \forall u,$$  \hspace{1cm} (10)

$Y$ is a deterministic function of $(U, X)$, i.e., we have

$$H(Y|U, X) = 0,$$  \hspace{1cm} (11)

and

$$|\mathcal{U}| \leq |\mathcal{X}|(|\mathcal{Y}| - 1) + 1.$$  \hspace{1cm} (12)

Proof. The proof is provided in [23, Appendix B].  \hfill \Box

Lemma 3. For any $0 \leq \epsilon < \sqrt{2I(X; Y)}$ and pair of RVs $(X, Y)$, there exists a RV $U$ supported on $\mathcal{U}$ such that $X$ and $U$ satisfy the strong privacy criterion 1, i.e., we have

$$d(P_{X,U}(\cdot, u), P_X P_U(u)) \leq \epsilon, \forall u,$$  \hspace{1cm} (13)

$Y$ is a deterministic function of $(U, X)$, i.e., we have

$$H(Y|U, X) = 0,$$  \hspace{1cm} (12)

$I(X; U|Y)$ can be upper bounded as follows

$$I(X; U|Y) \leq \alpha H(X|Y) + (1 - \alpha)\log(I(X; Y) + 1) + 4,$$  \hspace{1cm} (13)

and

$$|\mathcal{U}| \leq |\mathcal{X}|(|\mathcal{Y}| - 1) + 2 |\mathcal{X}| + 1,$$

where $\alpha = \frac{\epsilon^2}{2I(X)}$.

Proof. Let $U$ be found by ESFRF as in [9, Lemma 4], where we let the leakage be $\geq \epsilon$. The first constraint in this statement can be obtained by using the same proof as Lemma 2 and (13) can be derived using [9, Lemma 4].  \hfill \Box
REFERENCES

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

[2] I. Issa, S. Kamath, and A. B. Wagner, "An operational measure of information leakage," in 2016 Annual Conference on Information Science and Systems, March 2016, pp. 234–239.

[3] H. Wang, L. Vo, F. P. Calmon, M. Médard, K. R. Duffy, and M. Varia, “Privacy with estimation guarantees,” IEEE Transactions on Information Theory, vol. 65, no. 12, pp. 8025–8042, Dec 2019.

[4] H. Yamamoto, “A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers (corresp.),” IEEE Transactions on Information Theory, vol. 29, no. 6, pp. 918–923, 1983.

[5] B. Rassouli and D. Gündüz, “On perfect privacy,” IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 177–191, 2021.

[6] A. Zamani, T. J. Oechtering, and M. Skoglund, “A design framework for strongly $\chi^2$-private data disclosure,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2312–2325, 2021.

[7] A. Zamani, T. J. Oechtering, and M. Skoglund, “Data disclosure with non-zero leakage and non-invertible leakage matrix,” IEEE Transactions on Information Forensics and Security, vol. 17, pp. 165–179, 2022.

[8] Y. Y. Shkel, R. S. Blum, and H. V. Poor, “Secrecy by design with applications to privacy and compression,” IEEE Transactions on Information Theory, vol. 67, no. 2, pp. 824–843, 2021.

[9] A. Zamani, T. J. Oechtering, and M. Skoglund, “Bounds for privacy-utility trade-off with non-zero leakage,” arXiv preprint arXiv:2201.08738, 2022.

[10] C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” in Theory of cryptography conference. Springer, 2006, pp. 265–284.

[11] F. P. Calmon, A. Makhdoumi, M. Médard, M. Varia, M. Christiansen, and K. R. Duffy, “Principal inertia components and applications,” IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 5011–5038, Aug 2017.

[12] I. Issa, S. Kamath, and A. B. Wagner, “An operational approach to information leakage,” IEEE Transactions on Information Theory, vol. 66, no. 3, pp. 1625–1657, 2020.

[13] S. Asoodeh, M. Diaz, F. Alajaji, and T. Linder, “Estimation efficiency under privacy constraints,” IEEE Transactions on Information Theory, vol. 65, no. 3, pp. 1512–1534, 2019.

[14] B. Rassouli and D. Gündüz, “Optimal utility-privacy trade-off with total variation distance as a privacy measure,” IEEE Transactions on Information Forensics and Security, vol. 15, pp. 594–603, 2020.

[15] I. Issa, S. Kamath, and A. B. Wagner, “Maximal leakage minimization for the shannon cipher system,” in 2016 IEEE International Symposium on Information Theory, 2016, pp. 520–524.

[16] E. Erdemir, P. L. Dragotti, and D. Gündüz, “Active privacy-utility trade-off against inference in time-series data sharing,” arXiv preprint arXiv:2202.05833, 2022.

[17] F. P. Calmon and N. Fawaz, “Privacy against statistical inference,” in 2012 50th Annual Allerton Conference on Communication, Control, and Computing, Oct 2012, pp. 1401–1408.

[18] L. Sankar, S. R. Rajagopalan, and H. V. Poor, “Utility-privacy tradeoffs in databases: An information-theoretic approach,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 838–852, 2013.

[19] S. Sreekumar and D. Gündüz, “Optimal privacy-utility trade-off under a rate constraint,” in 2019 IEEE International Symposium on Information Theory, July 2019, pp. 2159–2163.

[20] Y. O. Basciftci, Y. Wang, and P. Ishwar, “On privacy-utility tradeoffs for constrained data release mechanisms,” in 2016 Information Theory and Applications Workshop, Jan 2016, pp. 1–6.

[21] Y. Wang, Y. O. Basciftci, and P. Ishwar, “Privacy-utility tradeoffs under constrained data release mechanisms,” arXiv preprint arXiv:1710.09295, 2017.

[22] C. T. Li and A. El Gamal, “Strong functional representation lemma and applications to coding theorems,” IEEE Transactions on Information Theory, vol. 64, no. 11, pp. 6967–6978, 2018.

[23] A. Zamani, T. J. Oechtering, and M. Skoglund, “Bounds for privacy-utility trade-off with per-letter privacy constraints and non-zero leakage,” arXiv preprint arXiv:2205.04881, 2022.

[24] I. Sason and S. Verdú, “$f$ -divergence inequalities,” IEEE Transactions on Information Theory, vol. 62, no. 11, pp. 5973–6006, 2016.