多级逐点泄漏约束下的隐私-效用权衡

1st AmirrezaZamani信息科学与工程系，*KTH*瑞典斯德哥尔摩 amizam@kth.se

2nd Parastoo Sadeghi工程与技术学院，*UNSW*澳大利亚堪培拉 p.sadeghi@unsw.edu.au

3rd MikaelSkoglund信息科学与工程系，*KTH*瑞典斯德哥尔摩 skoglund@kth.se

arXiv:2601.04815v1 [cs.IT] 8 Jan 2026

摘要

本文研究了一种信息论隐私机制设计：代理方观测到与私有数据 X相关的有用数据 Y。代理方希望向用户披露这些信息，因此利用隐私机制生成可披露的数据 U。我们假设代理方无法直接访问 X，即私有数据处于隐藏状态。我们研究的隐私机制设计旨在最大化关于 Y的披露信息量，该信息量通过 Y与 U之间的互信息来衡量，同时满足具有不同隐私泄漏预算的逐点约束。我们引入了一种称为多级逐点泄漏的新度量，它允许针对 U的不同实现值设定不同的泄漏级别。不同于以往关于逐点度量的研究（这些研究对每个实现值采用相同的泄漏级别），我们考虑了更一般的情形：每个数据点都可以在不同的阈值内泄漏信息。因此，这一概念还涵盖了某些数据点不应泄漏任何关于私有数据的信息的情况，即它们必须满足完美隐私。换言之，可以同时考虑完美隐私和非零泄漏。

当泄漏足够小时，信息几何中的概念使我们能够对互信息进行局部近似。我们证明，当泄漏矩阵 $P_{X|Y}$可逆时，利用这一近似可得到一个二次优化问题，并且在某些约束下该问题具有闭式解。具体而言，我们证明，只需考虑二元U 即可达到最优效用。由此可得到复杂度较低的简单隐私设计，其核心是求出一个矩阵的最大奇异值和奇异向量。随后，我们将方法推广到一般泄漏矩阵，并证明主要的复杂隐私-效用权衡问题可以近似为一个线性规划。最后，我们讨论如何扩大允许的泄漏范围。

索引词

逐点度量、多级泄漏、信息几何、局部近似。

I. 引言

在本文中，如图 1 所示，代理方希望向用户披露一些有用信息。我们用随机变量（RV） Y表示有用数据，它与用随机变量（RV） X表示的私有数据具有任意相关性。此外，RV U 表示代理方披露的披露数据。代理方的目标是基于 Y 设计 U，在满足逐点隐私准则的同时，尽可能多地披露有关 Y的信息。我们使用互信息衡量效用，并使用多级逐点约束衡量隐私泄漏。多级逐点泄漏度量对先前的逐点度量进行了推广，其特点是披露数据 U 的每个字母（实现值）都受不同隐私阈值的约束。该框架还涵盖完美隐私，即某些字母必须满足零泄漏约束。为说明我们的模型，我们考虑 U 的不同字母具有不同优先级的情形。例如，某些字母可能比其他字母更敏感。以临床研究为例，如果患者没有敏感疾病，披露这一信息可能不会造成伤害；然而，如果患者确实患有此类疾病，透露这一信息就可能导致隐私泄露。因此，相较于 U中较不敏感的结果，对 U 中更敏感的结果设定更严格的隐私条件是合理的。

A. 相关工作

关于信息论隐私机制设计的相关工作可见于 [1]–[25]。 [1],研究了将互信息同时用作隐私和效用度量时的隐私-效用权衡问题。在完美隐私假设下，研究表明，隐私机制设计问题可以归结为线性规划。在此，完美隐私对应于 U 与 X 完全独立，即从 X 到 U 中每个字母的泄漏都必须为零。 [2], 在完美保密假设下研究了设计保密问题。利用函数表示引理，推导出了安全分解的界限。 [3], 通过放宽完美保密约束并允许一定的泄漏，对 [2] 中考虑的隐私问题进行了推广。此外， [3] 中的界限在[22] 中利用分离技术得到了改进。

如 [4] 和 [5], 所述，使用平均度量来量化隐私泄漏可能并不理想，因为某些数据点（实现值）泄漏的信息可能超过预设阈值。换言之，如果对手能够访问这些字母，就可以推断出有关敏感数据 X的大量信息。例如，平均 χ^2 和 ℓ_1

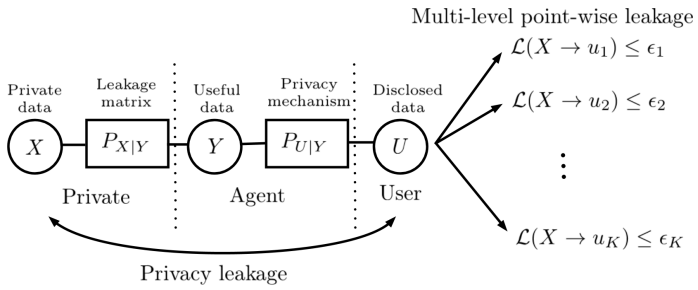

图 1. 在此模型中，披露数据 U 由隐私机制设计，该机制旨在最大化关于 Y 的信息披露量，同时满足多级逐点隐私约束。这里， U 的每个实现都必须满足具有不同泄漏预算的隐私约束。此外， $\mathcal{L}(X \to u_i)$表示从私有数据 X 到字母（实现） $u_i \in \mathcal{U}$的泄漏。

度量分别用于 [26] 和 [16], , 其中“平均”指对 U中的字母取平均。另一方面， χ^2 和 ℓ_1 分别在 [4] 和[5], 中通过引入逐点（强）隐私度量强化了这些概念。研究表明，利用信息几何中的概念，可以通过线性代数技术近似求解主要的复杂设计问题。提升这一概念对应另一种逐点度量，已在 [7] 中得到研究，它表示数据集中敏感特征的后验信念与先验信念之间的似然比。

信息几何中的概念已应用于各种网络信息论问题，以及隐私、保密性和公平性设计问题，用于近似复杂的优化问题并推导出简单的设计 [3]–[5], [19]–[21], [24], [27]–[30]。这些问题的主要挑战在于概率分布空间缺乏几何结构。假设我们关注的分布彼此接近，则 KL散度和互信息都可以用加权平方欧几里得距离近似。这带来了一种方法，可用于近似各种我们感兴趣的设计问题。

特别是，这种方法已用于研究 [27], [28],中的点对点信道和一些特定的广播信道。在隐私领域，该方法已用于 [3]–[5], [19]–[21], [24], , 其中 [21], 将互信息用作隐私度量，将相对熵用作效用度量，并且二者均以二次函数近似。在 [24], 中，隐私机制的设计采用 LIP 和最大提升作为隐私泄漏度量。此外， [29], [30] 使用该方法设计了满足有界人口统计均等和均等化赔率约束的公平机制。此外， [20], 利用信息几何对窃听信道的保密容量进行了局部近似。最后， [21], 也采用了类似方法，研究了由有界互信息定义的隐私泄漏约束下的假设检验问题。在高隐私区域，该问题可通过近似求解。

B. 主要贡献

需要强调的是，上述工作均未研究多级逐点隐私约束；也就是说，在所有先前的工作中， $\mathcal{L}(X \to u)$ 均由单一数值 ϵ 限定。正如上文所述，这构成了现有文献中的一个重要空白。在本文中，我们将研究结果分为以下两大部分。

1）可逆泄漏矩阵：在结果的第一部分，我们假设泄漏矩阵 $P_{X|Y}$ 可逆，并采用一种多层逐点 χ^2-隐私约束。该约束通过允许不同实现值 $u \in \mathcal{U}$具有不同的泄漏阈值，扩展了 [4] 中的度量。借助信息几何的概念，我们对主要的隐私–效用权衡问题进行近似，并将其转化为一个更简单的线性代数问题。当 U 为二元时，可推导出近似问题的闭式最优解。此外，在一般情形下，我们证明近似问题可化简为 U为二元的情形。换言之，无论 U的字母表大小如何，我们都可以在不失最优性的前提下，将 U限制为二元。这意味着在最优解中，只有泄漏阈值最高的两个字母表符号与 X相关联，而其他所有符号均不会泄露关于 X的任何信息。

2）一般泄漏矩阵：在结果的第二部分，我们首先假设泄漏矩阵 $P_{X|Y}$ 满行秩。此外，我们采用一种多层逐点 ℓ_1-隐私约束，通过允许不同实现值 $u \in \mathcal{U}$具有不同的泄漏预算，扩展了 [5] 。我们证明，主要问题的最优解位于某些凸多胞体的极点上。随后，我们使用泰勒展开近似主要问题在这些极点处的取值。最后，我们证明所得问题可化为一个线性规划。我们还讨论了如何将该框架推广到任意泄漏矩阵。

II. 系统模型与问题表述

令 P_{XY} 表示定义在有限字母表 $\mathcal{X}$ 和 $\mathcal{Y}$ 上的离散随机变量 X 和 Y 的联合分布。我们用定义在 $\mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|}$ 上的矩阵表示 P_{XY} , 并用定义在

$\mathbb{R}^{|\mathcal{X}|}$ 和 $\mathbb{R}^{|\mathcal{Y}|}$ 分别表示 P_{XY} 的行和与列和所得到的边缘分布向量。此外，我们用定义在 $\mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|}$ 上的矩阵表示泄漏矩阵 $P_{X|Y}$。此外，对于给定的 $u\in\mathcal{U}$，定义在 $\mathbb{R}^{|\mathcal{X}|}$ 上的 $P_{X,U}$（·、u）和 $P_{X|U}$（·|u）是分布向量，其元素分别为 $P_{X,U}$（x、u）和 $P_{X|U}$（$x|u$），对所有 $x\in\mathcal{X}$ 均成立。U 与 Y 之间的关系由定义在 $\mathbb{R}^{|\mathcal{U}|\times|\mathcal{Y}|}$ 上的核 $P_{U|Y}$ 描述。我们假设 U 的基数固定，且有 $|\mathcal{U}|=K$。本文中，P_X（x）、P_X、$\sqrt{P_X}$ 和 $[P_X]$ 分别表示 P_X（$X=x$）、X 的分布向量、元素为 $\sqrt{P_X}$（x）的向量，以及对角元素等于 P_X（x）的对角矩阵。对于两个大小相同的向量 P 和 Q，若对所有 x 均有 P（x）$\leq Q$（x），则称 $P\leq Q$。此外，我们假设代理方无法直接访问私有数据，因此形成马尔可夫链 $X-Y-U$。我们的目标是设计一种隐私机制，生成披露数据 U，在满足多级逐点隐私准则的同时最大化效用。本文使用互信息 I（U; Y）衡量效用，而隐私泄漏则由 $\mathcal{L}$（$X\to u_i$）$\triangleq D_f$（$P_{X|U=u_i}$; P_X）$\leq\epsilon_i$ 量化，其中对所有 $i\in\{1,\ldots,K\}$ 均有 $u_i\in\mathcal{U}$，而 D_f（P; Q）表示 P 与 Q 之间的一般 f-散度。因此，隐私问题可以表述如下

$$\sup_{P_{U|Y}} \quad I(U;Y), \tag{1a}$$
$$\text{subject to:} \quad X-Y-U, \tag{1b}$$
$$\mathcal{L}(X\to u_i)\leq\epsilon_i,\forall i\in\{1,\ldots,K\}, \tag{1c}$$

这里，我们假设 K 和 ϵ_i 值是固定的，且不失一般性，有 $\epsilon_1\geq\epsilon_2\geq\cdots\geq\epsilon_K\geq 0$.

注 1. 我们将 (1c) 称为多级逐点隐私约束，因为每个 u_i 都必须满足一个具有不同阈值的泄漏约束。此外，在本文中，我们假设已知 U的字母表，并设计滤波器 $P_{U|Y}$。该模型还涵盖一些 ϵ_i 值为零的混合情形。在 (1) 中令 $\epsilon_1=\ldots=\epsilon_K$ 和 $D_f(\cdot||\cdot)=\chi^2(\cdot||\cdot)$，即可得到 [4]中研究的问题。最后，令 $\epsilon_1=0$，该模型便简化为[1]中研究的完美隐私问题。

例 1. （启发性示例）考虑一个医疗数据集，其中私有数据 X 表示患者的确切诊断，有用数据 Y 包含临床测量数据，而披露数据 U 是向第三方发布的类别报告。U 的字母表可能包括诸如

$$u\in\{\text{“healthy”},\ \text{“low risk”},\ \text{“high risk”},\ \text{“critical”}\}.$$

由于这些结果的敏感性较低，泄露关于 X 的更多信息可能是允许的，例如披露 $U=$“健康”或 $U=$“低风险”。相比之下，出于伦理和法律考量，$U=$“高风险”或 $U=$“危急”必须满足严格得多的泄漏约束。因此，U 的不同取值对应不同的隐私泄漏阈值，自然形成多级逐点泄漏问题的表述。

A. 可逆的 $P_{X|Y}$:

这里，我们假设 $|\mathcal{X}|=|\mathcal{Y}|=N$ 和 $P_{X|Y}\in\mathbb{R}^{N\times N}$ 是可逆的。此外，我们选择 χ^2-距离作为式 (1) 中的 f-散度，并将主要问题表述如下。

$$g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY})\triangleq \sup_{\substack{P_{U|Y}:X-Y-U,\\ \chi^2(P_{X|u_i}||P_X)\leq\epsilon_i,\ \forall i\in\{1,\ldots,K\},}} I(Y;U), \tag{2}$$

注2. 令 (2) 中的 $\epsilon_1=\ldots=\epsilon_K$，即可得到 [4] 中研究的问题。此外，我们有

$$\begin{aligned} g^{\chi}_{\epsilon_K,\ldots,\epsilon_K}(P_{XY}) &\leq g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY})\\ &\leq g^{\chi}_{\epsilon_1,\ldots,\epsilon_1}(P_{XY}),\end{aligned}$$

其中，上界和下界在 [4] 中进行了研究。

B. 一般的 $P_{X|Y}$:

这里，我们首先假设 $P_{X|Y}$ 满行秩，且满足 $|\mathcal{X}|\leq|\mathcal{Y}|$。不失一般性，我们假设 $P_{X|Y}$ 可表示为两个子矩阵，其中第一个子矩阵可逆，即 $P_{X|Y}=[P_{X|Y_1},P_{X|Y_2}]$，使得定义在 $\mathbb{R}^{|\mathcal{X}|\times|\mathcal{X}|}$ 上的 $P_{X|Y_1}$ 可逆。我们选择 ℓ_1-距离作为式 (1) 中的 f-散度，并将主要问题表述如下。

$$g^{\ell}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY})\triangleq \sup_{\substack{P_{U|Y}:X-Y-U,\\ \ell_1(P_{X|u_i}||P_X)\leq\epsilon_i,\ \forall i\in\{1,\ldots,K\},}} I(Y;U), \tag{3}$$

注释 3. 将式 (3) 中的 $\epsilon_1 = \ldots = \epsilon_K$ 代入，可得到 [5] 中研究的问题。此外，我们有

$$\begin{aligned} g^{\ell}_{\epsilon_K,\ldots,\epsilon_K}(P_{XY}) &\le g^{\ell}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY}) \\ &\le g^{\ell}_{\epsilon_1,\ldots,\epsilon_1}(P_{XY}), \end{aligned}$$

其中，上界和下界已在 [5]中研究。

最后， 本文还讨论了如何将我们的框架推广到任意泄漏矩阵 .

III. Main Results

本节对（2）和（3）进行近似，并求解由此得到的优化问题。在陈述主要结果之前，我们将条件分布 $P_{X|U=u_i}$ P_X $u_i \in \mathcal{U}$ $P_{X|U=u_i}$ =改写为对 的扰动。因此，对于任意 ，$P_X + \epsilon_i \cdot J_{u_i}$ $J_{u_i} \in \mathbb{R}^{|\mathcal{X}|}$ 我们可以写作 ，其中 是一个满足以下性质的扰动向量。

$$\sum_{x\in\mathcal{X}} J_{u_i}(x) = 0,\ \forall u_i, \tag{4}$$

$$\sum_{i=1}^{K} \epsilon_i P_U(u_i) J_{u_i}(x) = 0,\ \forall x. \tag{5}$$

此外， $\forall u_i \in \{u$ $_1$，……， $u_K\}$，约束 $\chi^2(P_{X|u_i}||P_X) \le \epsilon_i$和 $\ell_1(P_{X|u_i}||P_X) \le \epsilon_i$可以改写为 as

$$\|[\sqrt{P_X}^{-1}]J_{u_i}\|_2 = \|L_{u_i}\|_2 \le 1,\ \forall u_i \in \{u_1,\ldots,u_K\}, \tag{6}$$

and

$$\|J_{u_i}\|_1 \le 1,\ \forall u_i \in \{u_1,\ldots,u_K\}, \tag{7}$$

分别地，其中 $L_{u_i} \triangleq [\sqrt{P_X}^{-1}]J_{u_i}$和 u_i是 U的第 i个字母表。

A. 可逆矩阵情形

在下一个结果中，我们用二次函数近似 (2)。为此，我们定义 $W \triangleq [\sqrt{P_Y}^{-1}]P^{-1}_{X|Y}[\sqrt{P_X}]$。在所有结果中，为简洁起见，均使用约束 $\sum_i P_U(u_i) = 1$，但不再显式写出。

命题1. 当 ϵ_1足够小时，(2) 可近似为以下问题

$$\max_{\substack{L_{u_i},P_U:\sum_i \epsilon_i P_U(u_i)L_{u_i}=0,\\ \|L_{u_i}\|_2\le 1,\ L_{u_i}\perp\sqrt{P_X},\forall i,}} 0.5\left(\sum_{i=1}^{K} P_U(u_i)\epsilon_i^2 \|WL_{u_i}\|^2\right). \tag{8}$$

证明. 证明与 [4] 类似，基于 KL散度的二阶泰勒近似。唯一的区别在于，由于存在多级泄漏约束，我们有

$$P_{X|U=u_i} = P_X + \epsilon_i \cdot J_{u_i},$$

这意味着

$$P_{Y|U=u_i} = P_Y + \epsilon_i P^{-1}_{X|Y} \cdot J_{u_i}.$$

接下来，我们近似互信息中出现的每一项 $D(P_{Y|U=u}||P_Y)$，其中 $D(\cdot||\cdot)$ 表示 KL 散度。

□

令 $\sigma_{\max}(W)$ 和 L^* 分别表示 W 的最大奇异值和对应向量，其中 $\|L^*\|_2 = 1$。在下一个结果中，我们针对二元 U 求解 (8)，即 $K = 2$。为简化记号，我们分别用 P_i 和 L_i 表示 $P_U(u_i)$ 和 L_{u_i}。

命题 2。对于 $K = 2$，有

$$(8) = \frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}(W), \tag{9}$$

由……达到

$$P_U(u_1) = \frac{\epsilon_2}{\epsilon_1+\epsilon_2},\ P_U(u_2) = \frac{\epsilon_1}{\epsilon_1+\epsilon_2}, \tag{10}$$

$$L_{u_1} = -L_{u_2} = L^*. \tag{11}$$

证明。 显然，(10) 和 (11) 满足 (8) 中的约束，因此得到一个可行候选解。此外，我们有

$$\frac{1}{2}\left(\sum_{u_i\in\{u_1,u_2\}}\epsilon_i^2 P_U(u_i)\|WL_{u_i}\|^2\right)=$$
$$\frac{1}{2}\sigma^2_{\max}(W)\left(\frac{\epsilon_1^2\epsilon_2}{\epsilon_1+\epsilon_2}+\frac{\epsilon_2^2\epsilon_1}{\epsilon_1+\epsilon_2}\right)=\frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}(W).$$

因此，(9) 是 (8) 的下界。接下来，我们证明它也是一个上界。利用约束 $P_1\epsilon_1 L_1+P_2\epsilon_2 L_2=0$，可得 $L_2=-\frac{P_1\epsilon_1}{P_2\epsilon_2}L_1$。将 L_2 代入 (8)，可将优化问题改写如下。

$$0.5\max_{\substack{L_1,P_1,P_2:\|L_1\|_2\le\min\{1,\frac{P_2\epsilon_2}{P_1\epsilon_1}\},\\ L_1\perp\sqrt{P_X},\ P_1+P_2=1,}} P_1\epsilon_1^2\|WL_1\|^2+\frac{P_1^2\epsilon_1^2}{P_2}\|WL_1\|^2$$
$$=0.5\epsilon_1^2\max_{\substack{L_1,P_1,P_2:\|L_1\|_2\le\min\{1,\frac{P_2\epsilon_2}{P_1\epsilon_1}\},\\ L_1\perp\sqrt{P_X},\ P_1+P_2=1,}}\frac{P_1}{P_2}\|WL_1\|^2 \tag{12}$$

其中，约束 $\|L_1\|_2\le\frac{P_2\epsilon_2}{P_1\epsilon_1}$ 由 $\|L_2\|_2\le 1$ 和 $L_2=-\frac{P_1\epsilon_1}{P_2\epsilon_2}L_1$ 推出。我们考虑两种情况：$\frac{P_2\epsilon_2}{P_1\epsilon_1}\ge 1\leftrightarrow P_1\le\frac{\epsilon_2}{\epsilon_1+\epsilon_2}$ 或 $\frac{P_2\epsilon_2}{P_1\epsilon_1}\le 1\leftrightarrow P_2\le\frac{\epsilon_1}{\epsilon_1+\epsilon_2}$。在第一种情况下，(12) 的上界如下。我们有

$$(12)=0.5\epsilon_1^2\max_{L_1,P_1:\|L_1\|_2\le 1,L_1\perp\sqrt{P_X},}\frac{P_1}{1-P_1}\|WL_1\|^2$$
$$\le 0.5\epsilon_1^2\sigma^2_{\max}\max_{P_1}\frac{P_1}{1-P_1}=0.5\epsilon_1\epsilon_2\sigma^2_{\max},$$

其中，在最后一行中，我们利用了 $\frac{P_1}{1-P_1}$ 是 P_1 的递增函数这一事实，因此选择 $P_1=\frac{\epsilon_2}{\epsilon_1+\epsilon_2}$。在第二种情况下，我们有

$$(12)=0.5\epsilon_1^2\max_{L_1,P_1,P_2:\|L_1\|_2\le\frac{P_2\epsilon_2}{P_1\epsilon_1},L_1\perp\sqrt{P_X},}\frac{P_1}{P_2}\|WL_1\|^2$$
$$\le 0.5\epsilon_2^2\sigma^2_{\max}\max_{P_2}\frac{P_2}{1-P_2}=0.5\epsilon_1\epsilon_2\sigma^2_{\max},$$

其中，最后一行是由

$$\frac{P_1}{P_2}\|WL_1\|^2\le\frac{P_1}{P_2}\sigma^2_{\max}\left(\frac{P_2\epsilon_2}{P_1\epsilon_1}\right)^2=\frac{P_2}{P_1}\sigma^2_{\max}(\frac{\epsilon_2}{\epsilon_1})^2.$$

在这两种情况下，上界均由 (10) 和 (11) 达到。因此，对于 $K=2$，我们有 (8) $=\frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}$。 □

接下来，我们证明，在求解 (8) 时不失最优性，可以假设 U 是二元的，并且在最高的两个泄漏阈值处具有非零泄漏，即 ϵ_1 和 ϵ_2。与命题 2 类似，为简化记号，我们用 P_i 和 L_i 表示 $P_U(u_i)$ 和 L_{u_i}。

引理 1. 求解(8)，不失最优性，我们可以假设 $K=2$，而对于 U 的其他字母，我们有

$$P_U(u_i)=0,\ i\ge 3.$$

换言之，我们有

$$(8)=0.5\max_{\substack{L_1,L_2,P_1,P_2:\|L_1\|_2,\|L_2\|_2\le 1,\\ L_1,L_2\perp\sqrt{P_X},\ P_1\epsilon_1L_1+P_2\epsilon_2L_2=0,}} P_1\epsilon_1^2\|WL_1\|^2+P_2\epsilon_2^2\|WL_2\|^2, \tag{13}$$

其中 $P_1+P_2=1$。

证明。 证明与 [4, 命题 4.] 类似。令 $\{L_u^*, P_U^*\}$ 为式 (8) 的最大化解，且 $\epsilon_1 \geq \epsilon_2 \geq \ldots \geq \epsilon_K$。此外，令 L_1^* 和 L_2^* 分别取得 $\|WL_{u_i}^*\|^2$的最高值和次高值，并令 u_m 和 u_n 为对应的字母。于是有

$$\begin{aligned}
&\sum_i \epsilon_i^2 P_U^*(u_i)\|WL_{u_i}^*\|^2 \\
&\overset{(a)}{\leq} \left(\sum_i \epsilon_i^2 P_U^*(u_i)\right)\|WL_1^*\|^2 + \left(\sum_j \epsilon_j^2 P_U^*(u_j)\right)\|WL_2^*\|^2 \\
&\overset{(b)}{\leq} \epsilon_1^2\left(\sum_i P_U^*(u_i)\right)\|WL_1^*\|^2 + \epsilon_2^2\left(\sum_j P_U^*(u_j)\right)\|WL_2^*\|^2 \\
&\overset{(c)}{=} \epsilon_1^2 P_1\|WL_1^*\|^2 + \epsilon_2^2 P_2\|WL_2^*\|^2,
\end{aligned}$$

其中，在步骤 (a) 中，我们将 U^* 的字母分为两组：第一组包含 u_m，第二组包含 u_n。其余字母随机选取。在步骤 (b) 中，我们使用 $\epsilon_1 \geq \epsilon_2 \geq \ldots \geq \epsilon_K$。最后，在步骤 (c) 中，令 $\sum_i P_U^*(u_i) = P_1$ 和 $\sum_j P_U^*(u_j) = P_2$，其中 $P_1 + P_2 = 1$。我们回顾一下，$\sum_i P_U^*(u_i) = P_1$ 对应于第一组的权重之和，该组包含 u_m；而 $\sum_j P_U^*(u_j) = P_2$ 表示第二组的权重之和，该组包含 u_n。换言之，m 包含在第一个求和式中，而 n 包含在第二个求和式中。由于最终的上界可由 (10) 和 (11) 达到，因此 (13) 得证。 □

推论 1. 如果 $\epsilon_3 < \epsilon_2$，则对于(8)的最大化解，有

$$P_U(u_3) = \ldots = P_U(u_K) = 0.$$

换言之，U 应当是一个二元随机变量，仅通过隐私预算最高的两个字母泄露关于 X 的信息。

证明。 该证明由引理 1 得出。设 $\epsilon_3 < \epsilon_2$。在这种情况下，如果存在 u_i，使得对于某个 $i \geq 3$，$P_U(u_i) > 0$，则 (b) 变为严格不等式。此外，由于最终上界是可达到的，任何满足对于某个 $i \geq 3$ 有 $P_U(u_i) > 0$ 的 U 所达到的效用，都严格小于由 (10) 和 (11) 达到的最终上界。证明完毕。 □

利用命题 1 和 2 以及引理 1，我们得到以下定理。在下一个结果中，近似记号$\simeq$ 对应于二阶泰勒展开。换言之，如果 $f(\epsilon) = g(\epsilon) + o(\epsilon^2)$，则 $f(\epsilon) \simeq g(\epsilon)$，其中 $o(\cdot)$ 表示巴赫曼–朗道记号。

定理 1. 当 ϵ_1足够小时，我们有

$$g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY}) \simeq (8) = \frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}(W). \tag{14}$$

等号在满足(10) 和(11)的二元 U 处成立。此外，当 $\epsilon_2 > \epsilon_3$时，使(8) 达到最大值的披露数据是一个二元随机变量，它仅通过隐私预算最高的两个字母泄露有关 X 的信息。

证明. 证明可由命题 1 和命题 2、引理 1 以及推论 1 得出。 □

求得 (8) 的优化器后，最终的隐私机制可表示为

$$P_{Y|U=u_1} = P_X + \epsilon_1 P_{X|Y}^{-1}[\sqrt{P_X}]L_{u_1}, \tag{15}$$

$$P_{Y|U=u_2} = P_X + \epsilon_2 P_{X|Y}^{-1}[\sqrt{P_X}]L_{u_2}. \tag{16}$$

此处，L_{u_1} 和 L_{u_2} 由 (11) 给出。此外，U 的边缘分布由 (10) 给出。**注 4.** 利用 *[4],*可得

$$\begin{aligned}
g^{\chi}_{\epsilon_1,\ldots,\epsilon_1}(P_{X,Y}) &\simeq \frac{1}{2}\epsilon_1^2\sigma^2_{\max}(W) \\
&\geq \frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}(W) \simeq g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY}).
\end{aligned}$$

此外，

$$\begin{aligned}
g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{X,Y}) &\simeq \frac{1}{2}\epsilon_1\epsilon_2\sigma^2_{\max}(W) \\
&\geq \frac{1}{2}\epsilon_K^2\sigma^2_{\max}(W) \simeq g^{\chi}_{\epsilon_K,\ldots,\epsilon_K}(P_{XY}).
\end{aligned}$$

推论 2. 由(10) 和(11)给出的(8)的优化器，导出了 $g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY})$ 的一个下界，如下所示：

$$g^{\chi}_{\epsilon_1,\ldots,\epsilon_K}(P_{XY}) \geq I(U^*;Y). \tag{17}$$

其中， $I(U^*;Y)$ 通过 隐私机制(15) 以及由(10给出的 U^* 的边缘分布进行评估).

证明。 证明基于以下事实：由 (15) 和 (10) 给出的隐私机制满足 (2) 中的约束。 □

B. 一般情形 $P_{X|Y}$

本节中，我们对 (3) 进行近似，并求解由此得到的优化问题。为此，我们首先考虑一个满行秩矩阵 $P_{X|Y}$。随后，我们讨论如何将其推广到任意矩阵。

与 [5], 类似，我们证明，对于满足 (3) 中约束的任意可行 U， $P_{Y|U=u_i}$ 均位于一个凸多胞体内。为此，令 $M \in \mathbb{R}^{|\mathcal{X}|\times|\mathcal{Y}|}$ 按如下方式构造：设 V 为 $P_{X|Y}$ 的右特征向量矩阵，即 $P_{X|Y} = U\Sigma V^T$ 和 $V = [v_1,\ v_2,\ ...,\ v_{|\mathcal{Y}|}]$，则 M 定义为

$$M \triangleq \left[v_1,\ v_2,\ ...,\ v_{|\mathcal{X}|}\right]^T. \tag{18}$$

引理 2. 设 J_{u_i} 满足性质 (4)、(5) 和 (7)。对于充分小的 $\epsilon > 0$，对任意 $u_i \in \mathcal{U}$，向量$P_{Y|U=u_i}$ 属于以下凸多胞体

$$\mathbb{S}_{u_i} = \left\{ y \in \mathbb{R}^{|\mathcal{Y}|} | My = MP_Y + \epsilon_i M \begin{bmatrix} P^{-1}_{X|Y_1} J_{u_i} \\ 0 \end{bmatrix},\ y \geq 0 \right\},$$

其中 $\begin{bmatrix} P^{-1}_{X|Y_1} J_{u_i} \\ 0 \end{bmatrix} \in \mathbb{R}^{|\mathcal{Y}|}$。

证明。 证明过程与 [5, 引理 2]类似，并基于 [5, 引理 1], 中给出的 M 零空间性质以及马尔可夫链 $X - Y - U$。唯一的区别是，对于每个向量 $P_{Y|U=u_i}$，我们使用不同的泄漏，即 ϵ_i。此外， J_{u_i}满足 (5)，其中包含一个额外项 ϵ_i。这不会影响证明。 □

接下来，类似于 [5, 定理 1] ，我们有以下等价性。我们不再最大化 $I(Y;U)$，而是最小化 $H(Y|U)$.

命题 3. 设 J_{u_i} 满足三个性质 (4)、(5) 和 (7)。我们有

$$\min_{\substack{P_{U|Y}:X-Y-U \\ \ell_1(P_{X|u_i}||P_X)\leq\epsilon_i,\ \forall u_i,}} H(Y|U) = \min_{\substack{P_U,\ P_{Y|U=u_i}\in\mathbb{S}_{u_i},\ \forall u_i\in\mathcal{U}, \\ \sum_i P_U(u_i)P_{Y|U=u_i}=P_Y, \\ J_{u_i}\ satisfies\ (4),\ (5),\ and\ (7)}} H(Y|U). \tag{19}$$

证明。 证明过程与 [5,定理 1]中的论证类似。 □

接下来，我们讨论如何对所有 $u_i \in \mathcal{U}$，在 $P_{Y|U=u_i} \in \mathbb{S}_{u_i}$上最小化 $H(Y|U)$。

命题 4 $P^*_{Y|U=u_i}\ \forall u_i \in \mathcal{U}$ $H\ Y|U$ $\{P_{Y|U=u_i} \in \mathbb{S}_{u_i},\ \forall u_i \in \mathcal{U} | \sum_i P_U\ u_i\ P_{Y|U=u_i} =$。 $P_Y\}$ $u_i \in \mathcal{U}$ $\mathbb{S}_{u_i}$
设，为在集合 () 上使 () 最小化的解，则对于所有， $P^*_{Y|U=u_i} \in \mathbb{S}_{u_i}$ 都必须属于 的极点。

证明。 证明过程与 [5, 命题 3] 类似，并基于熵的凹性。直观地说，如果 $P_{Y|U=u_i}$ 不是 $\mathbb{S}_{u_i}$的极点，则它可以表示为极点的凸组合。接着可以证明，熵$H(P_{Y|U=u_i})$可以降低。因此，对于每个 u_i，极小值点都属于 $\mathbb{S}_{u_i}$ 的极点。 □

按照 [5] 中相同的方法，我们可以求出极点，并近似计算（19）中的右端项。为求出 $\mathbb{S}_{u_i}$ 的极点，令 Ω_{u_i} 为一组指标，这些指标对应于 M 的 $|\mathcal{X}|$ 个线性无关列，即$|\Omega_{u_i}| = |\mathcal{X}|$ 和 $\Omega_{u_i} \subset \{1,..,|\mathcal{Y}|\}$。令 $M_{\Omega_{u_i}} \in \mathbb{R}^{|\mathcal{X}|\times|\mathcal{X}|}$ 为 M 的子矩阵，其列由集合 Ω_{u_i} 中的指标确定。假设 $\Omega_{u_i} = \{\omega_1,..,\omega_{|\mathcal{X}|}\}$，其中 $\omega_j \in \{1,..,|\mathcal{Y}|\}$，且所有元素均按升序排列。极点 $V^*{}_{\Omega^{u_i}}$ 的第 ω_j 个元素可由 $M^{-1}{}_{\Omega^{u_i}}(MP_Y + \epsilon_i M \begin{bmatrix} P^{-1}_{X|Y_1} J_{u_i} \\ 0 \end{bmatrix})$ 的第 j 个元素求得，即对于 $1 \leq j \leq |\mathcal{X}|$，

有

$$V^*_{\Omega_{u_i}}(\omega_j) = \left(M^{-1}_{\Omega_{u_i}} MP_Y + \epsilon_i M^{-1}_{\Omega_{u_i}} M \begin{bmatrix} P^{-1}_{X|Y_1} J_{u_i} \\ 0 \end{bmatrix} \right)(j). \tag{20}$$

$V^*\Omega^{u_i}$ 的其他元素均设为零。现在我们近似计算 $V^*\Omega^{u_i}$ 的熵。令 $V^*\Omega^{u_i}$ 为集合 $\mathbb{S}_u$ 的一个极点，则有

$$\begin{aligned} H(P_{Y|U=u_i}) &= \sum_{y=1}^{|\mathcal{Y}|} -P_{Y|U=u}(y)\log(P_{Y|U=u}(y)) \\ &= -(b_{u_i} + \epsilon_i a_{u_i} J_{u_i}) + o(\epsilon_i), \end{aligned} \tag{21}$$

with

$$\begin{aligned} b_{u_i} &= l_{u_i}\left(M_{\Omega_{u_i}}^{-1} M P_Y\right), \\ a_{u_i} &= l_{u_i}\left(M_{\Omega_{u_i}}^{-1} M(1:|\mathcal{X}|) P_{X|Y_1}^{-1}\right) \in \mathbb{R}^{1\times|\mathcal{X}|}, \\ l_{u_i} &= \left[\log\left(M_{\Omega_u}^{-1} M P_Y(j)\right)\right]_{j=1:|\mathcal{X}|} \in \mathbb{R}^{1\times|\mathcal{X}|}, \end{aligned}$$

并且， $M^{-1}\Omega_{u_i} MP_Y(j)$表示向量 $M^{-1}\Omega_{u_i} MP_Y$中的第 j个（$1 \le j \le |\mathcal{X}|$）元素。此外， $M(1:|\mathcal{X}|)$表示 M的子矩阵，其包含前 $|\mathcal{X}|$列。(21)的证明与 [5,引理 4]类似，并基于对$\log(1+x)$进行一阶泰勒展开。利用(21)，我们可以将(19)近似为如下形式。

定理 2. 当 ϵ_1充分小时，(19)中的最小化问题可近似为如下形式

$$\begin{aligned} &\min_{P_U(.),\{J_{u_i},u_i\in\mathcal{U}\}} -\left(\sum_{i=1}^{K} P_U(u_i)(b_{u_i} + \epsilon_i a_{u_i} J_{u_i})\right), \\ &\textit{subject to:} \\ &\sum_{i=1}^{K} P_U(u_i) V_{\Omega_{u_i}}^* = P_Y,\ \sum_{i=1}^{K} P_U(u_i)\epsilon_i J_{u_i} = 0,\ P_U \in \mathbb{R}_+^K, \\ &\|J_{u_i}\|_1 \le 1,\ \mathbf{1}^T \cdot J_{u_i} = 0,\ \forall u_i \in \mathcal{U}. \end{aligned} \tag{22}$$

此外，(22) 可以改写为线性规划。

证明. (22)的证明可直接由(21)以及 $H(Y|U)$的最小值在集合 $\mathbb{S}_{u_i}$的极点处取得这一事实得出。为证明该定理的第二个结论，我们注意到，利用向量

$$\eta_{u_i} = P_U(u_i)\left(M_{\Omega_{u_i}}^{-1} M P_Y + \epsilon_i M_{\Omega_{u_i}}^{-1} M(1:|\mathcal{X}|) P_{X|Y_1}^{-1} J_{u_i}\right)$$

对于所有 $u_i \in \mathcal{U}$，其中$\eta_{u_i} \in \mathbb{R}^{|\mathcal{X}|}$，我们可以将(22)写成线性规划。向量$\eta_{u_i}$ 对应于极点 $V^*\Omega^{u_i}$中的非零元素个数的倍数。此外， $P_U(u_i)$和 J_{u_i}可以唯一确定为

$$\begin{aligned} P_U(u_i) &= \mathbf{1}^T \cdot \eta_{u_i}, \\ J_{u_i} &= \frac{P_{X|Y_1} M(1:|\mathcal{X}|)^{-1} M_{\Omega_{u_i}} [\eta_{u_i} - (\mathbf{1}^T \eta_{u_i}) M_{\Omega_{u_i}}^{-1} M P_Y]}{\epsilon_i (\mathbf{1}^T \cdot \eta_{u_i})}. \end{aligned}$$

接下来，我们利用（22）和 η_{u_i} 求得线性规划。对于代价函数，我们有

$$\begin{aligned} &-\left(\sum_{i=1}^{K} P_U(u_i) b_{u_i} + \epsilon_i P_U(u_i) a_{u_i} J_{u_i}\right) = -\sum_i b_i (\mathbf{1}^T \eta_{u_i}) \\ &-\epsilon_i \sum_i a_{u_i}\left[P_{X|Y_1} M(1:|\mathcal{X}|)^{-1} M_{\Omega_{u_i}} [\eta_{u_i} - (\mathbf{1}^T \eta_{u_i}) M_{\Omega_{u_i}}^{-1} M P_Y]\right], \end{aligned}$$

对于所有 $u_i \in \mathcal{U}$，它都是 η_{u_i} 中元素的线性函数。向量 $P_U(u_i)V^*\Omega^{u_i}$ 的非零元素等于 η_{u_i}中的元素，即我们有

$$P_U(u_i) V_{\Omega_{u_i}}^*(\omega_j) = \eta_{u_i}(j).$$

因此，约束 $\sum_{i=1}^{K} P_U(u_i)V^*_{\Omega_{u_i}} = P_Y$ 可以改写为 η_{u_i} 中元素的线性函数。对于约束 $\sum_{i=1}^{K} \epsilon_i P_U(u_i) J_{u_i} = 0$、$P_U(u_i) \geq 0$，$\forall u_i$，和 $\sum_{j=1}^{|\mathcal{X}|} J_{u_i}(x_j) = 0$，我们有

$$\begin{aligned}
&\sum_i P_{X|Y_1} M(1:|\mathcal{X}|)^{-1} M_{\Omega_{u_i}} \left[\eta_{u_i} - (\mathbf{1}^T \cdot \eta_{u_i}) M^{-1}_{\Omega_{u_i}} M P_Y\right] = 0,\\
&\sum_j \eta_{u_i}(j) \geq 0,\ \forall u_i \in \mathcal{U},\\
&\mathbf{1}^T P_{X|Y_1} M(1:|\mathcal{X}|)^{-1} M_{\Omega_{u_i}} \left[\eta_{u_i} - (\mathbf{1}^T \cdot \eta_{u_i}) M^{-1}_{\Omega_{u_i}} M P_Y\right] = 0.
\end{aligned}$$

此外，对于最后一个约束 $\sum_j |J_{u_i}(x_j)| \leq 1$，我们有

$$\begin{aligned}
&\sum_j \left| \left(P_{X|Y_1} M(1:|\mathcal{X}|)^{-1} M_{\Omega_{u_i}} \left[\eta_{u_i} - (\mathbf{1}^T \eta_{u_i}) M^{-1}_{\Omega_{u_i}} M P_Y\right]\right)(j) \right| \leq\\
&\epsilon_{u_i} (\mathbf{1}^T \eta_{u_i}),\ \forall u_i \in \mathcal{U}.
\end{aligned}$$

最后一个约束包含绝对值，可以通过分别考虑每个绝对值的两种情形来处理。因此，对于所有 u_i，所有约束都可以改写为关于 η_{u_i} 中元素的线性函数。 □

IV. Discussions

本节首先讨论混合情形，其中 U 的某些字母满足完美隐私。然后讨论如何将该框架扩展到任意矩阵 $P_{X|Y}$。

A. 混合情形

本部分讨论部分隐私预算为零的情形，也就是某些字母满足完美隐私的情形。为此，令 $\epsilon_1 \geq \cdots \geq \epsilon_t \geq \epsilon_{t+1} = \cdots = \epsilon_K = 0$，即字母 $\{u_{t+1}, \ldots, u_K\}$ 满足完美隐私。在这种情况下，对于所有 $u \in \{u_{t+1}, \ldots, u_K\}$，引理 2 中的凸多胞体为

$$\mathbb{S}_{u_i} = \left\{ y \in \mathbb{R}^{|\mathcal{Y}|} | My = MP_Y,\ y \geq 0 \right\}. \tag{23}$$

此外，对于 $u_i \in \{u_{t+1}, \ldots, u_K\}$，(20) 中的极点变为

$$V^*_{\Omega_{u_i}}(\omega_j) = \left(M^{-1}_{\Omega} M P_Y\right)(j).$$

我们注意到，对于这类字母，我们不近似熵 $H(P_{Y|U=u_i})$，并得到以下结果。

定理 3. 设 $\epsilon_1 \geq \cdots \geq \epsilon_t \geq \epsilon_{t+1} = \cdots = \epsilon_K = 0$。当 ϵ_1 足够小时，(19) 中的最小化问题可近似为如下形式

$$\begin{aligned}
&\min_{P_U(.), \{J_{u_i}, u_i \in \mathcal{U}_1\}} -\left(\sum_{i=1}^{K} P_U(u_i) b_{u_i} + \sum_{i=1}^{t} P_U(u_i) \epsilon_i a_{u_i} J_{u_i} \right) \qquad (24)\\
&\textit{subject to:}\\
&\sum_{i=1}^{K} P_U(u_i) V^*_{\Omega_{u_i}} = P_Y,\ \sum_{i=1}^{t} P_U(u_i) \epsilon_i J_{u_i} = 0,\ P_U \in \mathbb{R}^K_+,\\
&\|J_{u_i}\|_1 \leq 1,\ \mathbf{1}^T \cdot J_{u_i} = 0,\ \forall u_i \in \mathcal{U}_1.
\end{aligned}$$

其中 $\mathcal{U}_1 = \{u_1, \ldots, u_t\}$。此外，(24) 可改写为一个线性规划。

证明。 证明过程与定理 2 类似。唯一的区别是，对于 $u_i \in \{u_{t+1}, \ldots, u_K\}$，我们不近似熵 $H(Y|U = u_i)$。此外，对于这些字母，熵等于 b_{u_i}。对于线性规划，我们对 $u_i \in \mathcal{U}_1$ 使用与定理 2 中相同的变换。对于 U 的其余实现值，我们使用

$$\eta_{u_i} = P_U(u_i) \left(M^{-1}_{\Omega_{u_i}} M P_Y \right).$$

□

注 5。 与可逆情形不同，在混合情形中，零泄漏的字母仍可在效用项中取得非零权重，即 $P_U(u_i) > 0$ 即使 $P_{X|U=u_i} = P_X$。更多详情请参阅数值示例。

B. 推广到任意 $P_{X|Y}$

这里，我们讨论如何将用于近似（3）的框架推广到任意 $P_{X|Y}$。通过检查 [5,引理 2], 的证明，我们发现凸多胞体 $\mathbb{S}_{u_i}$ 由以下方程得出:

$$P_{X|U=u_i} - P_X = P_{X|Y}\left[P_{Y|U=u_i} - P_Y\right] = \epsilon_i J_{u_i}. \tag{25}$$

当 $P_{X|Y}$ 满行秩时，我们可以使用其可逆子矩阵 $P_{X|Y_1}$ 求得一个特解，并使用其余部分描述落在 $P_{X|Y}$的零空间中的分量。然而，对于一般的 $P_{X|Y}$，我们可以改用 $P_{X|Y}$ 的伪逆来求特解。具体而言，由（25）可得

$$P_{Y|U=u_i} = P_Y + \epsilon_i P_{X|Y}^{\dagger} J_{u_i} + z^*, \tag{26}$$

其中， $P_{X|Y}^{\dagger}$是 $P_{X|Y}$的伪逆， $z^* \in \text{null}(P_{X|Y})$。与满行秩情形的主要区别在于，这里的项 $\epsilon_i P_{X|Y}^{\dagger} J_{u_i}$充当特解，而不是

$$\epsilon_i \begin{bmatrix} P_{X|Y_1}^{-1} J_{u_i} \\ 0 \end{bmatrix}.$$

然后，利用 M 矩阵在 [5,引理 1],中给出的性质，我们得到以下结果 t.

引理 3. 设 J_{u_i} 满足三个性质 (4)、(5) 和 (7)。对于充分小的 $\epsilon_1 > 0$，对每个 $u_i \in \mathcal{U}$，向量$P_{Y|U=u_i}$ 属于以下凸多胞体

$$\mathbb{S}_{u_i} = \left\{ y \in \mathbb{R}^{|\mathcal{Y}|} | My = MP_Y + \epsilon_i M P_{X|Y}^{\dagger} J_{u_i},\ y \geq 0 \right\}.$$

按照前文所述的相同步骤， $\mathbb{S}_{u_i}$ 的极点为

$$V^*_{\Omega_{u_i}}(\omega_j) = \left(M_{\Omega_{u_i}}^{-1} M P_Y + \epsilon_i M_{\Omega_{u_i}}^{-1} M P_{X|Y}^{\dagger} J_{u_i} \right)(j). \tag{27}$$

此外， $V^*\Omega(\omega_i)$ 的熵可近似表示如下

$$H(P_{Y|U=u}) \simeq -(b_{u_i} + \epsilon_i a'_{u_i} J_{u_i}), \tag{28}$$

with

$$b_{u_i} = l_{u_i}\left(M_{\Omega_{u_i}}^{-1} M P_Y \right),$$

$$a'_{u_i} = l_{u_i}\left(M_{\Omega_{u_i}}^{-1} M P_{X|Y}^{\dagger} \right) \in \mathbb{R}^{1\times|\mathcal{X}|},$$

$$l_{u_i} = \left[\log\left(M_{\Omega_{u_i}}^{-1} M P_Y(j) \right) \right]_{j=1:|\mathcal{X}|} \in \mathbb{R}^{1\times|\mathcal{X}|}.$$

注意，在证明近似 [5, 引理 4], 中的极点时，我们用到了以下事实:

$$1^T M_{\Omega_{u_i}}^{-1} M(1:|\mathcal{X}|) P_{X|Y_1}^{-1} = 0.$$

这里，对伪逆的扩展同样成立。具体而言，我们需要证明

$$1^T M_{\Omega_{u_i}}^{-1} M P_{X|Y}^{\dagger} = 0.$$

使用与 [5, 引理 4], 中相同的论证，只需证明

$$1^T P_{X|Y}^{\dagger} = 1^T.$$

这由.....可得

$$1^T = 1^T I = 1^T P_{X|Y} P_{X|Y}^{\dagger} = 1^T P_{X|Y}^{\dagger},$$

其中我们使用了 $P_{X|Y} P_{X|Y}^{\dagger} = I$和 $1^T P_{X|Y} = 1^T$。更多详情请参见 [5, 引理 4]。因此，我们将定理 2 扩展如下。

定理 4. 对于任意泄漏矩阵 $P_{X|Y}$ 以及足够小的 ϵ_1，(19)中的最小化问题可近似表示如下

$$\min_{P_U(.),\{J_{u_i},u_i\in\mathcal{U}\}} -\left(\sum_{i=1}^{K} P_U(u_i)(b_{u_i}+\epsilon_i a'_{u_i}J_{u_i})\right) \tag{29}$$

subject to:

$$\sum_{i=1}^{K} P_U(u_i)V^*_{\Omega_{u_i}} = P_Y,\ \sum_{i=1}^{K} P_U(u_i)\epsilon_i J_{u_i} = 0,\ P_U\in\mathbb{R}_+^K,$$

$$\|J_{u_i}\|_1 \le 1,\ \mathbf{1}^T\cdot J_{u_i} = 0,\ \forall u_i\in\mathcal{U}.$$

此外，(29) 可以改写为一个线性规划。

证明。 证明过程与定理 3 中的论证类似。唯一的区别是，我们使用 (27) 而不是 (20)，并使用 a'_{u_i} 而不是 a_{u_i}。

□

注 6。 我们强调，在 (26) 中，我们使用 $Ax = b$的通解。然而，有些情况下该系统无解。例如，如果 b 不属于 A的列空间，那么就不存在满足 $Ax = b$的 x 。在这种情况下， $A^\dagger b$ 使 $\|Ax - b\|$最小化。

为了解决这一问题，我们按照上述步骤求解相应的线性规划。得到J_{u_i}后，我们检查是否满足(25) 。如果(25) 不满足，则表明可行集为空，无法实现非零效用。

当 $P_{X|Y}$是高矩阵时，也就是当 $|\mathcal{X}| > |\mathcal{Y}|$时，可能出现这种情况。然而在实践中，我们通常有 $|\mathcal{X}| < |\mathcal{Y}|$。本文提出的框架适用于可行集非空的情况。具体而言，我们忽略(3) $= 0$的情况。

C. 扩大允许的泄漏范围

本节讨论如何将我们的方法应用于更大的允许泄漏区间。本文中，为了近似$I(U; Y)$，我们在凸多胞体 $\mathbb{S}_{u_i}$ 的极点处，对 $\log(1 + x)$ 使用一阶泰勒展开。扩大允许泄漏区间的一种方法是对 $\log(1 + x)$ 使用高阶近似。这是因为高阶泰勒展开能够在更大的 x 范围内达到相同的近似误差。具体而言，如果一阶近似在区间 $x \le c_1$ 内有效，那么高阶近似可以在区间$x \le c_2$内有效，其中 $c_2 > c_1$，同时保持相同的近似误差。例如，设

$$\log(1+x) = x - \frac{x^2}{2} + \text{error}_1(x),$$

and

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \text{error}_2(x).$$

如果第一种近似使用区间 $x \le c_1$，那么第二种近似可以使用区间 $x \le c_2$ ，其中 $c_2 > c_1$，以达到相同的误差，即

$$|\text{error}_1(x)| = |\text{error}_2(x)|.$$

此外，与现有结果相比，我们得到了更紧的界（更接近最优值）；但优化问题也变得更加复杂。

V. Numerical Example

这里，我们采用 [5,示例 2]，并将我们在多级隐私约束下的设计与其进行比较。我们研究如下混合情形。令 $P_{X|Y} = \begin{bmatrix}0.3 & 0.8 & 0.5 & 0.4\\ 0.7 & 0.2 & 0.5 & 0.6\end{bmatrix}$ 和 $P_Y = [\frac{1}{2},\ \frac{1}{4},\ \frac{1}{8},\ \frac{1}{8}]^T$。此外，令 $\epsilon_1 = \epsilon_2 = \epsilon_3 = 0.01$和 $\epsilon_4 = 0$。令

$J_{u_i} = \begin{bmatrix} J^1_{u_i} \\ J^2_{u_i} \end{bmatrix}$ 对于 $u_i \in \{u_1, u_2, u_3\}$。利用（4），我们得到 $J^1_{u_i} + J^2_{u_i} = 0$。因此，我们通过 $\begin{bmatrix} -J^2_{u_i} \\ J^2_{u_i} \end{bmatrix}$ 展示 J_{u_i}。对于 $u_i \in \{u_1, u_2, u_3\}$， $\mathbb{S}_{u_i}$ 的极点如下

$$V^*_{1_{\Omega_{u_i}}} = \begin{bmatrix} 0.675 - 2\epsilon_i J^2_{u_i} \\ 0.325 + 2\epsilon_i J^2_{u_i} \\ 0 \\ 0 \end{bmatrix}, \; V^*_{2_{\Omega_{u_i}}} = \begin{bmatrix} 0.1875 + 5\epsilon_i J^2_{u_i} \\ 0 \\ 0.8125 - 5\epsilon_i J^2_{u_i} \\ 0 \end{bmatrix}$$

$$V^*_{3_{\Omega_{u_i}}} = \begin{bmatrix} 0 \\ 0.1563 - 2.5\epsilon_i J^2_{u_i} \\ 0 \\ 0.8437 + 2.5\epsilon_i J^2_{u_i} \end{bmatrix}, \; V^*_{4_{\Omega_{u_i}}} = \begin{bmatrix} 0 \\ 0 \\ 0.6251 - 10\epsilon_i J^2_{u_i} \\ 0.3749 + 10\epsilon_i J^2_{u_i} \end{bmatrix},$$

其中 $\epsilon_i = 0.01$。 $u_i = u_4$ 的极点集合如下

$$V^*_{1_{\Omega_{u_4}}} = \begin{bmatrix} 0.675 \\ 0.325 \\ 0 \\ 0 \end{bmatrix}, \; V^*_{2_{\Omega_{u_4}}} = \begin{bmatrix} 0.1875 \\ 0 \\ 0.8125 \\ 0 \end{bmatrix}$$

$$V^*_{3_{\Omega_{u_4}}} = \begin{bmatrix} 0 \\ 0.1563 \\ 0 \\ 0.8437 \end{bmatrix}, \; V^*_{4_{\Omega_{u_4}}} = \begin{bmatrix} 0 \\ 0 \\ 0.6251 \\ 0.3749 \end{bmatrix}.$$

检查所有可能的极点组合后（其中大多数不可行），我们选择 $\mathbb{S}_{u_1}$ 的第四个极点、$\mathbb{S}_{u_2}$ 的第二个极点、$\mathbb{S}_{u_3}$ 的第三个极点以及 $\mathbb{S}_{u_4}$ 的第一个极点。为简化符号，我们分别用 J_i 和 P_i 表示 J_{u_i} 和 $P_U(u_i)$。因此，我们得到以下问题

$$\begin{aligned}
\min \; & P_1 0.9544 + P_2 0.6962 + P_3 0.6254 + P_4 0.9097 \\
& + P_1 \epsilon J_1^2 7.3747 + P_2 \epsilon J_2^2 10.5816 - P_3 \epsilon J_3^2 6.0808 \\
\text{s.t.} \; & \begin{bmatrix} \frac{1}{2} \\ \frac{1}{4} \\ \frac{1}{8} \\ \frac{1}{8} \end{bmatrix} = P_1 \begin{bmatrix} 0 \\ 0 \\ 0.6251 - 10\epsilon J_1^2 \\ 0.3749 + 10\epsilon J_1^2 \end{bmatrix} + P_2 \begin{bmatrix} 0.1875 + 5\epsilon J_2^2 \\ 0 \\ 0.8125 - 5\epsilon J_2^2 \\ 0 \end{bmatrix} \\
& + P_3 \begin{bmatrix} 0 \\ 0.1563 - 2.5\epsilon J_3^2 \\ 0 \\ 0.8437 + 2.5\epsilon J_3^2 \end{bmatrix} + P_4 \begin{bmatrix} 0.675 \\ 0.325 \\ 0 \\ 0 \end{bmatrix}, \\
& P_1 J_1^2 + P_2 J_2^2 + P_3 J_3^2 = 0, \; P_1, P_2, P_3, P_4 \geq 0, \\
& |J_1^2| \leq \frac{1}{2}, \; |J_2^2| \leq \frac{1}{2}, \; |J_3^2| \leq \frac{1}{2},
\end{aligned}$$

其中，最小化的变量为 $P_U(u)$ 和 J_u^2，且 $\epsilon = 0.01$。接下来，我们将该问题转化为线性规划。我们有

$$\begin{aligned}
\eta_1 &= \begin{bmatrix} 0.6251 P_1 - 10\epsilon P_1 J_1^2 \\ 0.3749 P_1 + 10\epsilon P_1 J_1^2 \end{bmatrix} = \begin{bmatrix} \eta_1^1 \\ \eta_1^2 \end{bmatrix}, \\
\eta_2 &= \begin{bmatrix} 0.1875 P_2 + 5\epsilon P_2 J_2^2 \\ 0.8125 P_2 - 5\epsilon P_2 J_2^2 \end{bmatrix} = \begin{bmatrix} \eta_2^1 \\ \eta_2^2 \end{bmatrix}, \\
\eta_3 &= \begin{bmatrix} 0.1563 P_3 - 2.5\epsilon P_3 J_3^2 \\ 0.8437 P_3 + 2.5\epsilon P_3 J_3^2 \end{bmatrix} = \begin{bmatrix} \eta_3^1 \\ \eta_3^2 \end{bmatrix}, \\
\eta_4 &= P_4.
\end{aligned}$$

线性规划可表示为

$$
\begin{aligned}
\min\ & 0.6779\eta_1^1 + 1.4155\eta_1^2 + 2.415\eta_2^1 + 0.2995\eta_2^2 \\
& 2.6776\eta_3^1 + 0.2452\eta_3^2 + 0.9097\eta_4 \\
\text{s.t. } & \begin{bmatrix} \frac{1}{2} \\ \frac{1}{4} \\ \frac{1}{8} \\ \frac{1}{8} \end{bmatrix} = \begin{bmatrix} 0.675\eta_4 + \eta_2^1 \\ 0.325\eta_4 + \eta_3^1 \\ \eta_2^2 + \eta_1^1 \\ \eta_3^2 + \eta_1^2 \end{bmatrix}, \begin{cases} \eta_1^1 + \eta_1^2 & \geq 0 \\ \eta_2^1 + \eta_2^2 & \geq 0 \\ \eta_3^1 + \eta_3^2 & \geq 0 \\ \eta_4 & \geq 0 \end{cases} \\
& \frac{0.6251\eta_1^2 - 0.3749\eta_1^1}{10} + \frac{0.8125\eta_2^1 - 0.1875\eta_2^2}{5} + \\
& \frac{0.1563\eta_3^2 - 0.8437\eta_3^1}{2.5} = 0, \\
& \frac{|0.6251\eta_1^2 - 0.3749\eta_1^1|}{\eta_1^1 + \eta_1^2} \leq 5\epsilon, \\
& \frac{|0.8125\eta_2^1 - 0.1875\eta_2^2|}{\eta_2^1 + \eta_2^2} \leq 2.5\epsilon, \\
& \frac{|0.1563\eta_3^2 - 0.8437\eta_3^1|}{\eta_3^1 + \eta_3^2} \leq 1.125\epsilon.
\end{aligned}
$$

由此可得

$$
P_U = \begin{bmatrix} 0 \\ 0.1488 \\ 0.143 \\ 0.7082 \end{bmatrix},
$$

并且我们得到 $I(U;Y) \cong 0.9109$，其小于 [5] 中达到的效用，同时大于 [1] 中完美隐私情形下的效用。这是因为在本例中，我们强制 u_4 满足完美隐私。此外，与可逆矩阵 $P_{X|Y}$ 的情形不同，此处虽然 $\epsilon_4 = 0$，我们仍为 u_4 得到非零权重，即 $P_U(u_4) = 0.7082 > 0$。这印证了注释 3。

VI. 结论

本文研究了不同逐点泄漏约束下的信息论隐私机制设计。我们提出了多级逐点泄漏的概念，通过允许不同披露输出具有不同的泄漏预算，对现有逐点泄漏度量进行了推广，同时也涵盖了完美隐私与非零泄漏的混合情形。对于小泄漏区域，我们利用信息几何近似，得到了隐私–效用权衡的可处理闭式形式。特别是，我们证明，当泄漏矩阵可逆时，所得问题具有二次形式且存在闭式解；此外，二元披露数据足以实现最优效用。我们还通过线性规划近似，将该方法推广到一般泄漏矩阵，并讨论了扩展允许泄漏范围的方法。这些结果为具有多级泄漏控制的隐私机制设计提供了灵活且计算高效的框架。最后，受本文模型启发，还可以考虑其他若干研究方向。一个有趣的问题是在 X 的字母表上定义泄漏度量，即 $\mathcal{L}(x_i \to U) \leq \epsilon_i$。在这种情况下，可以采用类似的方法得到闭式解。此外，我们还可以考虑这样一种情形：从 X 字母表中的每个符号到 U 字母表中每个符号的泄漏均有界，即 $\mathcal{L}(x_i \to u_j) \leq \epsilon_{i,\,j}$。在这种情况下，可以考虑局部差分隐私、LIP 和提升度等度量。这些方向留待未来研究。

参考文献

[1] B. Rassouli 和 D. G¨und¨uz, 《论完美隐私》, IEEE 信息论精选领域期刊, 第 2 卷, 第 1 期, 第 177–191 页, 2021 年。[2] Y. Y. Shkel、R. S. Blum 和 H. V. Poor, 《以设计实现保密: 在隐私与压缩中的应用》, IEEE 信息论汇刊, 第 67 卷, 第 2 期, 第 824–843 页, 2021 年。[3] A. Zamani、T. J. Oechtering 和 M. Skoglund, 《直接访问与不直接访问私有数据时的隐私-效用权衡》, IEEE 信息论汇刊, 第 70 卷, 第 3 期, 第 2177–2200 页, 2024 年。[4] ——, 《强

χ^2 16, 2312 2325, 隐私

2021

数据披露的设计框架》, IEEE 信息取证与安全汇刊, 第 卷, 第 页 – 。[5] A. Zamani、T. J. Oechtering 和 M. Skoglund, 《具有非零泄漏和不可逆泄漏矩阵的数据披露》, IEEE 信息取证与安全汇刊, 第 17 卷, 第 165–179 页, 2022 年。[6] M. A. Zarrabian 和 P. Sadeghi, 《一种在隐私漏斗及其他基于提升度的度量中改善隐私-效用权衡的算法》, 载于 2024 年第 17 届信号处理与通信系统国际会议 (ICSPCS), 2024 年, 第 1–7 页。[7] M. A. Zarrabian 、 N. Ding 和 P. Sadeghi, 《论提升度、相关隐私度量及其在隐私 – 效用权衡中的应用》, Entropy, 第 25 卷, 第 4 期, 第 679 页, 2023 年。[8] B. Jiang、M. Seif、R. Tandon 和 M. Li, 《上下文感知的局部信息隐私》, IEEE 信息取证与安全汇刊, 第 16 卷, 第 3694–3708 页, 2021 年。[9] J. C. Duchi、M. I. Jordan 和 M. J. Wainwright, 《局部隐私与统计极小极大速率》, 载于 2013 年 IEEE 第 54 届计算机科学基础年会。IEEE, 2013 年, 第 429–438 页。[10] P. Kairouz、S. Oh 和 P. Viswanath, 《局部差分隐私的极值机制》, 神经信息处理系统进展, 第 27 卷, 2014 年。[11] A. Evfimievski、J. Gehrke 和 R. Srikant, 《限制隐私保护数据挖掘中的隐私泄露》, 载于第二十二届 ACM SIGMOD-SIGACT-SIGART 数据库系统原理研讨会论文集, 2003 年, 第 211–222 页。[12] P. Kairouz、S. Oh 和 P. Viswanath, 《差分隐私的组合定理》, 载于国际机器学习会议。PMLR, 2015 年, 第 1376–1385 页。[13] G. Barthe 和 F. Olmedo, 《超越差分隐私: 概率程序之间 f-散度的组合定理与关系逻辑》, 载于自动机、语言与编程国际学术讨论会。Springer, 2013 年, 第 49–60 页。[14] V. Feldman、I. Mironov、K. Talwar 和 A. Thakurta, 《迭代隐私放大》, 载于 2018 年 IEEE 第 59 届计算机科学基础年会 (FOCS)。IEEE, 2018 年, 第 521–532 页。[15] A. Makhdoumi、S. Salamatian、N. Fawaz 和 M. M´edard, 《从信息瓶颈到隐私漏斗》, 载于 2014 年 IEEE 信息论研讨会, 2014 年, 第 501–505 页。[16] B. Rassouli 和 D. G¨und¨uz, 《以全变差距离作为隐私度量时的最优效用-隐私权衡》, IEEE 信息取证与安全汇刊, 第 15 卷, 第 594–603 页, 2020 年。[17] F. P. Calmon 和 N. Fawaz, 《针对统计推断的隐私保护》, 载于 2012 年第 50 届阿勒顿通信、控制与计算年会, 2012 年 10 月, 第 1401–1408 页。[18] E. Erdemir、P. L. Dragotti 和 D. G¨und¨uz, 《时间序列数据共享中针对推断的主动隐私-效用权衡》, IEEE 信息论精选领域期刊, 第 4 卷, 第 159–173 页, 2023 年。[19] B. Razeghi、F. P. Calmon、D. G¨und¨uz 和 S. Voloshynovskiy, 《论完美混淆: 局部信息几何分析》, 载于 2020 年 IEEE 信息取证与安全国际研讨会, 2020 年, 第 1–6 页。[20] E. M. Athanasakos、N. Kalouptsidis 和 H. Manjunath, 《保密容量的局部近似》, 载于 2024 年第 32 届欧洲信号处理会议 (EUSIPCO), 2024 年, 第 745–749 页。[21] J. Liao、L. Sankar、V. Y. F. Tan 和 F. du Pin Calmon, 《高隐私区域中互信息隐私约束下的假设检验》, IEEE 信息取证与安全汇刊, 第 13 卷, 第 4 期, 第 1058–1071 页, 2018 年。[22] A. Zamani、T. J. Oechtering 和 M. Skoglund, 《采用分离技术的统计隐私机制设计》, 载于 2024 年第 32 届欧洲信号处理会议 (EUSIPCO), 2024 年, 第 735–739 页。[23] M. Lopuha¨a-Zwakenberg、H. Tong 和 B. ˇSkori´c, 《具有差分隐私保证的隐私漏斗数据净化协议》, International Journal on Advances in Security, 第 13 卷, 第 3&4 期, 第 162–174 页, 2021 年。[24] A. Zamani、P. Sadeghi 和 M. Skoglund, 《局部信息隐私的信息几何方法及其在最大提升度和局部差分隐私中的应用》, 载于 2025 年 IEEE 信息论研讨会 (ITW), 2025 年, 第 1–6 页。[25] V. Yachongka 和 R. A. Chou, 《分布式数据库中的隐私约束有损函数计算》, 载于 2025 年 IEEE 信息论国际研讨会 (ISIT), 2025 年, 第 1–6 页。[26] H. Wang、L. Vo、F. P. Calmon、M. M´edard、K. R. Duffy 和 M. Varia, 《具有估计保证的隐私保护》, IEEE 信息论汇刊, 第 65 卷, 第 12 期, 第 8025–8042 页, 2019 年 12 月。[27] S. Borade 和 L. Zheng, 《欧几里得信息论》, 载于 2008 年 IEEE 苏黎世国际通信研讨会, 2008 年, 第 14–17 页。[28] S. L. Huang 和 L. Zheng, 《线性信息耦合问题》, 载于 2012 年 IEEE 信息论国际研讨会论文集。IEEE, 2012 年, 第 1029–1033 页。[29] A. Zamani、A. ¨Ozg

¨ *2512 00135*, ur 和

2025

M. Skoglund, 《采用信息几何方法研究具有均等化赔率约束的公平性》, arXiv 预印本 arXiv: . .[30] ——, 《具有有界逐点统计均等约束的公平性信息论研究: 一种信息几何方法》, arXiv 预印本 arXiv:2511.22683, 2025 年。