关于提升、相关隐私度量及其在隐私-效用权衡中的应用

Mohammad Amin Zarrabian、Ni Ding 和 Parastoo Sadeghi。

arXiv:2303.01017v1 [cs.IT] 2 Mar 2023

摘要

本文研究提升，即数据集中敏感特征的后验信念与先验信念之间的似然比。敏感特征上的最大提升和最小提升量化了对手的知识增益，为保护隐私，应对其加以限制。我们证明，最大提升和最小提升具有不同的取值范围和在数据集中出现的概率，这一现象称为提升不对称性。我们提出非对称局部信息隐私（ALIP），作为一种与提升不对称性相容的隐私概念，在该概念下，可对最小提升和最大提升施加不同的界限。我们将 ALIP 用于看门狗机制和最优随机响应（ORR）机制，这两种机制是实现基于提升的隐私的主要方法。结果表明，与现有的局部信息隐私相比，ALIP 在这些方法中能提升效用；现有局部信息隐私对最大提升和最小提升施加相同（对称）的界限。我们提出用于看门狗机制的子集合并方法，以提高数据效用；并提出用于 ORR 的子集随机响应方法，以降低复杂度。随后，我们研究了相关的基于提升的度量，包括 ℓ_1-范数、 χ^2-隐私准则和 α-提升。我们发现，这些度量只能限制最大提升，从而导致显著的最小提升泄漏。为解决这一问题，我们提出相应的提升逆度量来限制最小提升。我们将这些基于提升和提升逆的度量应用于看门狗机制。结果表明，它们可视为 ALIP 的松弛形式：只需限制平均最大提升和平均最小提升，便能实现更高的效用。

I. 引言

随着“大数据”时代的到来，通信系统和机器学习方法的发展推动了数据的生成、共享和分析日益普及。共享数据集对于实现社会和经济效益至关重要，但可能导致私人信息泄漏，这引发了人们对个人隐私保护的高度关注。保护隐私的主要方法是通过隐私机制扰动数据。考虑一些以随机变量 X 表示的原始数据，以及以 S表示的敏感特征，两者通过联合分布$P_{SX} \neq P_S \times P_X$相关联。应用隐私机制（由转移概率 $P_{Y|X}$表征），将 Y发布为 X 的净化版本，以保护 S。

隐私机制的设计取决于隐私度量。差分隐私（DP） [1]–[3] 是一种广泛使用的隐私概念。DP 限制推断某个个体是否存在于数据集中的可能性。它通过将后验信念 $P_{Y|S}(y|s)/P_{Y|S}(y|s')$之比限制在阈值 e^{ε}. 以下，确保仅有一条记录不同的相邻敏感特征 s 和 s'产生相似的输出概率分布。在局部差分隐私（LDP） [4]–[8], 中，邻接假设被放宽：对于任意两个敏感特征s 和 s'，后验信念之比均被限制在 e^{ε} 以下，这称为 ε-LDP。 ε 的量称为隐私预算。DP 和 LDP 被视为与上下文无关的隐私概念，即它们不考虑先验分布 P_S。相比之下，信息论（IT）隐私（亦称上下文感知隐私） [9], [10], 假设数据分布或其估计值是可用的。一些主要的信息论隐私度量包括互信息（MI） [9], [11], [12], 、最大泄露 [13]–[15]、 α-泄漏 [16],以及局部信息隐私（LIP） [10], [17]–[27]。一个挑战在于，数据扰动虽然限制了隐私泄漏，却必然会降低数据分辨率和数据集的实用性。因此，我们希望隐私机制能够提供令人满意的数据效用水平。根据应用场景，数据效用可通过衡量 X 与Y相似度的指标量化，例如 f散度 [6] 和互信息（MI） [6], [11], ；也可通过衡量差异和误差的指标量化，例如汉明失真 [7], [8] 和均方误差 [21], 。隐私与效用之间的这种矛盾称为隐私-效用权衡（PUT）。

本文研究提升，它是信息论隐私度量中的一个关键要素，指数据集中关于敏感特征的后验信念 $P_{S|Y}(s|y)$ 与先验信念 $P_S(s)$ 之间的似然比：

$$l(s,y) = \frac{P_{S|Y}(s|y)}{P_S(s)} = \frac{P_{SY}(s,y)}{P_S(s)P_Y(y)}. \tag{1}$$

提升 $i(s,y)$ 的对数 $=\log l(s,y)$，我们称之为对数提升，是信息密度 [23]。对于每个 y，$P_{S|Y}(s|y)$ 与 $P_S(s)$ 的差异越大，对手从 s 中获得的知识就越多。因此，最小提升和最大提升，

M. A. Zarrabian 任职于澳大利亚堪培拉的澳大利亚国立大学工程、计算与控制论学院，电子邮箱：moham- mad.zarrabian@anu.edu.au。N. Ding 任职于澳大利亚墨尔本的墨尔本大学计算与信息系统学院，电子邮箱：ni.ding@unimelb.edu.au。P. Sadeghi 任职于澳大利亚堪培拉的新南威尔士大学工程与信息技术学院，电子邮箱：p.sadeghi@unsw.edu.au。本研究的初步结果曾部分发表于 2022年 IEEE声学、语音与信号处理国际会议以及 IEEE 信息论研讨会。

分别记为 $\min_s l(s,y)$ 和 $\max_s l(s,y)$，用于量化每个 y 的最高隐私泄漏。在 LIP 中，最小提升和最大提升分别受下限阈值 $e^{-\varepsilon}$ 和上限阈值 e^{ε} 的约束，以限制对手的知识增益，记为 ε-LIP。实现 ε-LIP 的主要隐私机制包括看门狗机制 [23], [24] 和最优随机响应（ORR） [27]。看门狗机制将 X 的字母表划分为低风险符号和高风险符号，仅对高风险符号进行随机化。已有研究证明，在 [24] 中， X 不变随机化（例如合并所有高风险符号）可使看门狗机制的隐私泄漏最小化。ORR 是一种用于 ε-LIP 的最优机制，可将互信息（MI）这一效用度量最大化。

A. 主要贡献

我们研究了提升及其相关隐私概念，例如 LIP。我们证明，最小提升和最大提升在数据集中的取值及出现概率各不相同。具体而言，最小提升的取值范围比最大提升更广，而最大提升在数据集中出现的可能性更高 $P_{SY}(s,y)$。我们将这一性质称为提升不对称性。然而， ε-LIP 为 $\min_s i(s,y)$ 和 $\max_s i(s,y)$ 分配对称隐私预算（分别记为 $-\varepsilon$ 和 ε），这与提升不对称性不相容。因此，我们提出非对称局部信息隐私（ALIP），将其作为一种适用于提升性质的隐私概念；该概念可为 $\min_s i(s,y)$ 和 $\max_s i(s,y)$ 分配非对称隐私预算，分别记为 $-\varepsilon_l$ 和 ε_u。我们证明，ALIP 蕴含 ε-LDP，并且在 watchdog 和 ORR 机制中能够比 LIP 获得更好的效用。放宽对最小提升的界限可以提高效用，因为最小提升在数据集中出现的概率较低。

我们提出两种随机化方法，以克服看门狗机制效用低和 ORR 机制复杂度高的问题。在看门狗机制中， X不变随机化会同时扰动所有高风险符号，从而降低数据分辨率和效用。另一方面，ORR 的复杂度很高，且随数据集规模呈指数增长。为解决这些问题，我们提出子集合并和子集随机响应（SRR）扰动方法，将高风险符号划分为更细的子集，并分别对每个子集进行隐私保护。子集合并通过对互不相交的高风险符号子集应用 X不变随机化，提升看门狗机制的效用。此外，SRR 通过对互不相交的高风险符号子集应用随机响应方案，降低 ORR 在大型数据集上的复杂度，并实现近最优效用。

除了 LIP，我们还考虑了近期提出的一些隐私度量，称为基于提升的度量，包括 ℓ_1-范数[28]、 χ^2-强隐私 [29], 和 α-提升 [30]。这些度量被提出作为比各自对应的平均泄漏更强的隐私概念，分别对应全变差距离 [31]、 χ^2-散度 [32], 和 Sibson互信息 [15], [30], 。我们指出，这些度量只能界定最大提升泄漏，却可能导致显著的最小提升泄漏。因此，我们提出这些度量相应的修订版本，以限制最小提升泄漏，并称之为提升逆度量。我们在看门狗机制中结合子集合并随机化，应用基于提升和提升逆的度量，以研究其 PUT。由于这些度量是敏感特征上的平均提升函数，因此其效用高于 ALIP；也就是说，它们可以视为对最大和最小提升的放宽。

II. 预备知识

A. 符号约定

本文中统一使用以下符号约定。大写字母表示离散随机变量，对应的大写花体字母表示其有限支撑集，小写字母表示它们的任一取值。例如，随机变量 X的支撑集为 $\mathcal{X}$，其取值为 $x \in \mathcal{X}$。对于随机变量 S和 X，我们用 P_{SX}表示它们的联合概率分布，用 $P_{S|X}$ 表示给定 X时 S 的条件分布，用 P_S 和 P_X 表示它们的边缘分布。粗体大写和小写字母分别表示矩阵和向量，而小写字母表示向量的相应元素，例如 $\mathbf{v} = [v_1, v_2, \cdots, v_n]^T$。我们还用 $|\cdot|$表示集合的基数，例如 $|\mathcal{X}|$。自然对数记作 log，整数集 $\{1, 2, \cdots, n\}$ 记作 $[n]$。指示函数记作 $\mathbf{1}_{\{f\}}$；当 f 为真时，其值为 1，否则为 0。

B. 系统模型与隐私度量

考虑要共享的一些有用数据，记为随机变量 X ，其字母表为 $\mathcal{X}$。它与一些敏感特征 S 相关，这些特征的字母表为 $\mathcal{S}$ ，二者通过离散联合分布 P_{SX} 关联。为保护敏感特征，使用隐私机制生成 X 的净化版本，记为 Y ，其字母表为 $\mathcal{Y}$。我们假设 P_S 和 P_X 均具有全支撑，并且 $P_{Y|X,\ S}(y|x,s) = P_{Y|X}(y|x)$，由此得到马尔可夫链 $S - X - Y$。

主要的隐私度量是提升[1], , 如式（1）所示。提升及其对数——对数提升——量化了通过访问 $y \in \mathcal{Y}$而在每个敏感特征 $s \in \mathcal{S}$ 上获得的乘法信息增益。有两种情况： $l(s,y) > 1 \Rightarrow P_{S|Y}(s|y) > P_S(s)$ 表示发布 y后，对 s 的信念有所增强； $l(s,y) \leq 1 \Rightarrow P_{S|Y}(s|y) \leq P_S(s)$ 则表示发布 y 会降低信念。后验信念偏离先验信念越多，对手关于 s获得的知识就越多。因此，对于每个 $y \in \mathcal{Y}$,

[1]由于我们假设 P_S 和 P_Y 都具有全支撑，因此 $l(s,y)$ 是有限的。

$\max_s l(s,y)$ 和 $\min_s l(s,y)$ 决定了敏感特征的最大知识增益，应对它们加以限制以保护隐私。我们对这些量采用以下符号约定：

$$\Psi(y) \triangleq \min_{s\in\mathcal{S}} l(s,y) \quad \text{and} \quad \Lambda(y) \triangleq \max_{s\in\mathcal{S}} l(s,y). \tag{2}$$

提升已应用于局部信息隐私 [23], [24], [27] 中，以保护敏感特征，其定义如下。

定义1。对于 $\varepsilon \in \mathbb{R}_+$，若隐私机制 $\mathcal{M}: \mathcal{X} \to \mathcal{Y}$ 相对于 S是 ε-局部信息隐私或 ε-LIP，则对于所有 $y \in \mathcal{Y}$,

$$\mathrm{e}^{-\varepsilon} \le \Psi(y) \quad \textit{and} \quad \Lambda(y) \le \mathrm{e}^{\varepsilon}. \tag{3}$$

另一种逐实例度量是局部差分隐私 [4], [5], [27],

定义2。对于 $\varepsilon \in \mathbb{R}_+$，若隐私机制 $\mathcal{M}: \mathcal{X} \to \mathcal{Y}$ 相对于 S是 ε-局部差分隐私或 ε-LDP，则对于所有 s、$s' \in \mathcal{S}$ 以及所有 $y \in \mathcal{Y}$,

$$\Gamma(y) = \sup_{s,s'\in\mathcal{S}} \frac{P_{Y|S}(y|s)}{P_{Y|S}(y|s')} = \frac{\Lambda(y)}{\Psi(y)} \le \mathrm{e}^{\varepsilon}. \tag{4}$$

III. 非对称局部信息隐私

根据（3），LIP通过对称界限制了$\log \Psi(y)$的减小量和$\log \Lambda(y)$的增加量。然而，我们证明，这些度量在数据集 $P_{SY}(s,y)$中具有明显不同的取值范围和出现概率。我们在图1中绘制了 10^3 个随机生成的分布下$\log\ \Psi(y)$和$\log\ \Lambda(y)$的直方图，其中 $|\mathcal{X}| = 17$ 和$|\mathcal{S}| = 5$。在该图中，$\log\ \Psi(y)$的取值范围为 $[-12, -0.06]$，远大于$\log\ \Lambda(y)$的取值范围 $[0.02, 1.64]$。此外，$\log \Psi(y)$的最大概率远低于$\log\ \Lambda(y)$的最大概率。我们将这些性质称为提升不对称性。由于较高取值的 $|\log\ \Psi(y)|$ 的出现概率[2] 显著低于$\log\ \Lambda(y)$，因此我们可以通过为最小提升隐私分配更高的隐私预算来放宽其限制，同时对最大提升采用更严格的界。由此，我们提出了非对称局部信息隐私（ALIP），其中分别为 $|\log\ \Psi(y)|$和$\log \Lambda(y)$考虑不同的隐私预算 ε_l 和 ε_u。

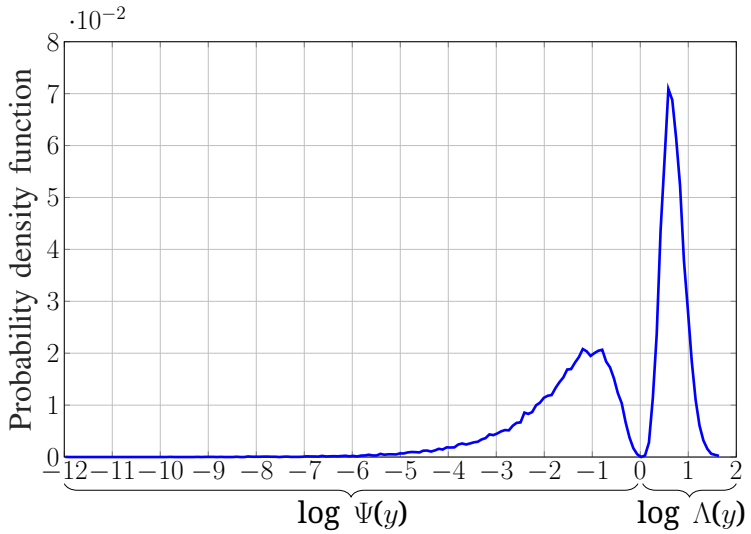


图 1：对于 10^3 个随机生成的分布，$\log\ \Psi(y) = \min_s i(s,y)$ 和 $\log\ \Lambda(y) = \max_s i(s,y)$ 的直方图，其中$|\mathcal{X}| = 17$、$|\mathcal{S}| = 5$。

这将产生以下隐私概念，与提升不对称性更加兼容。

定义 3。对于 ε_l、$\varepsilon_u \in \mathbb{R}_+$，隐私机制 $\mathcal{M}: \mathcal{X} \to \mathcal{Y}$ 关于 S，如果对所有 $y \in \mathcal{Y}$，则称其为（ε_l，ε_u）-非对称局部互信息隐私，或（ε_l，ε_u）-ALIP，

$$\mathrm{e}^{-\varepsilon_l} \le \Psi(y) \quad \textit{and} \quad \Lambda(y) \le \mathrm{e}^{\varepsilon_u}. \tag{5}$$

以下 p　　该命题说明了 $(\varepsilon_l, \varepsilon_u)$-ALIP 如何限制平均隐私泄漏度量和 LDP　　.

[2]例如，在图1中，$|\log\ \Psi(y)| \ge 6$ 的概率接近于零。

命题 1. 如果满足 $(\varepsilon_l, \varepsilon_u)$-ALIP，则，

1) $I(S;Y) \le \varepsilon_u$,2 $T\ S\ Y\ \le \frac{1}{2}\ ^{\varepsilon_u} - 1$ $\chi^2\ S\ Y\ \le\ ^{\varepsilon_u} - 1\ ^2$,) (;) (e) 和 (;) (e)) $I_\alpha^S(;) \le \frac{\alpha}{\alpha-1}\varepsilon_u$ 和 $I_\alpha^A(;) \le \frac{\alpha}{\alpha-1}\varepsilon_u$, 4) 满足 ε-LDP，其中 $\varepsilon = \varepsilon_l + \varepsilon_u$,

其中， $T(S;\ Y)$ 是全变差距离， $\chi^2(S;\ Y)$ 是 χ^2-散度， $I_\alpha^S(S;\ Y)$ 是 Sibson互信息，而 $I_\alpha^A(S;\ Y)$ 是 Arimoto互信息。

证明。证明见附录 A。 □

命题 1-1 至 1-3 表明，平均度量受最大提升隐私预算所界定。在 III-A 小节中，我们展示了 ALIP 可以通过放宽最小提升 $\varepsilon_l > \varepsilon_u$ 来提高效用，同时在命题 1 中为最大提升和平均度量设置较小的上界。命题 1-4 展示了 $(\varepsilon_l, \varepsilon_u)$-ALIP 与 ε-LDP 之间的关系。我们引入变量 $\lambda \in (0, 1)$，以便如下方便地表示这种关系：对于 LDP 隐私预算 ε，若设定 $\varepsilon_l = \lambda\varepsilon$ 和 $\varepsilon_u = (1-\lambda)\varepsilon$，则有 $\varepsilon_l + \varepsilon_u = \varepsilon$。因此，改变 λ 即可在相同的 ε-LDP 预算下产生不同的 $(\varepsilon_l, \varepsilon_u)$-ALIP 情形。若 $\lambda < 0.5$，则放宽最大提升隐私；若 $\lambda > 0.5$，则意味着放宽最小提升隐私。当 $\lambda = 0.5$ 时，我们得到 $\frac{\varepsilon}{2}$-LIP 的对称情形，其中 $\varepsilon_l = \varepsilon_u = \frac{\varepsilon}{2}$。

A. ALIP隐私-效用权衡

在本小节中，我们提出一种基于 ALIP 和 LDP 的看门狗机制，以及一种用于 ALIP 的非对称 ORR（AORR）机制，以扰动数据并实现隐私保护。我们考察 ALIP 和 LDP 的 PUT，其中效用通过 X 与 Y, $I(X;Y)$ 之间的互信息来衡量。

1) 看门狗机制：看门狗隐私机制将 $\mathcal{X}$ 划分为低风险子集和高风险子集，分别记为 $\mathcal{X}_L$和 $\mathcal{X}_H$，并且仅对高风险符号进行随机化。在现有的 LIP 中， $\mathcal{X}_L$ 和 $\mathcal{X}_H$ 由对称界确定。我们提出使用 ALIP 来获得 $\mathcal{X}_L$ 和 $\mathcal{X}_H$:

$$\mathcal{X}_L \triangleq \{x \in \mathcal{X} : \mathrm{e}^{-\varepsilon_l} \le \Psi(x) \quad and \quad \Lambda(x) \le \mathrm{e}^{\varepsilon_u}\} \quad and \quad \mathcal{X}_H = \mathcal{X} \setminus \mathcal{X}_L. \tag{6}$$

对于 LDP， $\mathcal{X}_L$ 和 $\mathcal{X}_H$ 由下式给出

$$\mathcal{X}_L \triangleq \{x \in \mathcal{X} : \Gamma(x) \le \mathrm{e}^{\varepsilon}\} \quad and \quad \mathcal{X}_H = \mathcal{X} \setminus \mathcal{X}_L. \tag{7}$$

获得 $\mathcal{X}_L$ 和 $\mathcal{X}_H$后，隐私机制为

$$\mathcal{M} = \begin{cases} \mathbf{1}_{\{x=y\}}, & x, y \in \mathcal{X}_L = \mathcal{Y}_L, \\ r(y|x), & x \in \mathcal{X}_H, y \in \mathcal{Y}_H, \\ 0, & \text{otherwise}, \end{cases} \tag{8}$$

其中， $\mathbf{1}_{\{x=y\}}$ 表示不加改动地发布低风险符号，而 $r(y|x)$ 表示对高风险符号进行随机化，其中 $\sum_{y\in\mathcal{Y}_H} r(y|x) = 1$。

一种 $r(y|x)$ 的实例是 X-不变随机化，即对于 $x \in \mathcal{X}_H, y \in \mathcal{Y}_H$， $r(y|x) = \mathcal{R}(y)$，且 $\sum_{y\in\mathcal{Y}_H} \mathcal{R}(y) = 1$。 $\mathcal{R}(y)$ 的一个例子是均匀随机化 $\mathcal{R}(y) = \frac{1}{|\mathcal{Y}_H|}$，其特殊情形为完全合并： $|\mathcal{Y}_H| = 1$，并且所有 $x \in \mathcal{X}_H$ 都映射到一个超符号 $y^* \in \mathcal{Y}_H$。已有研究 [24] 证明，对于 LIP， X-不变随机化可使 $\mathcal{X}_H$ 中的隐私泄漏最小。因此，如果我们在看门狗机制中应用 ALIP，对于 $\mathcal{X}_H \neq \varnothing$，在 $\mathcal{X}_H$ 上的最小泄漏为

$$\overline{\varepsilon}_u := \max_{s\in\mathcal{S}} i(s, \mathcal{X}_H) = \max_{s\in\mathcal{S}} \log l(s, \mathcal{X}_H) = \max_{s\in\mathcal{S}} \log \frac{P(\mathcal{X}_H|s)}{P(\mathcal{X}_H)}, \tag{9}$$

$$\overline{\varepsilon}_l := \left|\min_{s\in\mathcal{S}} i(s, \mathcal{X}_H)\right| = \left|\min_{s\in\mathcal{S}} \log l(s, \mathcal{X}_H)\right| = \left|\min_{s\in\mathcal{S}} \log \frac{P(\mathcal{X}_H|s)}{P(\mathcal{X}_H)}\right|, \tag{10}$$

其中 $P(\mathcal{X}_H|s) = \sum_{x\in\mathcal{X}_H} P_{X|S}(x|s)$，且 $P(\mathcal{X}_H) = \sum_{x\in\mathcal{X}_H} P_X(x)$。

X不变随机化同样适用于 LDP，以下定理表明，它在 $\mathcal{X}_H$ 中使 LDP 隐私泄漏最小化。

定理1。在 LDP 看门狗机制中， $\mathcal{X}_L$ 和 $\mathcal{X}_H$ 根据 (7) 确定时， X不变随机化使 $\mathcal{X}_H$ 中的隐私泄漏最小化，该泄漏由 (4) 中的 $\Gamma(y)$ 衡量。

证明。证明见附录B。 □

在采用 X 不变随机化的看门狗机制中，由 X 和 Y 之间的互信息度量的效用为

$$I(X;Y) = H(X) - \sum_{x\in\mathcal{X}_H} P_X(x)\log\frac{P(\mathcal{X}_H)}{P_X(x)}. \tag{11}$$

在 [24], 中，已验证式 (11) 中的 $I(X;Y)$ 关于 $\mathcal{X}_H$ 是单调的：如果 $\mathcal{X}_H^{'} \subset \mathcal{X}_H$，则 $I(X;Y) < I^{'}(X;Y)$，其中 $I^{'}(X;Y)$ 是 $\mathcal{X}_H^{'}$ 所得到的效用。

命题2. 在具有 X-不变随机化的看门狗机制中，对于给定的 LDP 隐私预算 ε、$\lambda \in (0,1)$ 以及 ALIP 隐私预算 $\varepsilon_l = \lambda\varepsilon$、$\varepsilon_u = (1-\lambda)\varepsilon$，LDP 所得到的效用高于 ALIP。

证明. 记 LDP 的高风险子集为 $\mathcal{X}_H^{'}$，ALIP 的高风险子集为 $\mathcal{X}_H$。根据式 (11) 后的注释，只需证明 $\mathcal{X}_H^{'} \subseteq \mathcal{X}_H$。我们有

$$\mathcal{X}_H^{'} = \{x\in\mathcal{X} : \frac{\Lambda(x)}{\Psi(x)} > \varepsilon\} \quad \text{and} \quad \mathcal{X}_H = \{x\in\mathcal{X} : \Lambda(x) > \mathrm{e}^{(1-\lambda)\varepsilon} \ \ or \ \ \Psi(x) < \mathrm{e}^{-\lambda\varepsilon}\}.$$

如果 $x\in\mathcal{X}_H^{'}$，则 $\Lambda(x) > \mathrm{e}^{(1-\lambda)\varepsilon}$ 或 $\Lambda(x) \le \mathrm{e}^{(1-\lambda)\varepsilon}$。若前者成立，则 $x\in\mathcal{X}_H$。若后者成立，由于 $\frac{\Lambda(x)\ \Psi(x)}{} > \mathrm{e}^{\varepsilon}$，我们得到 $\Lambda(x) > \mathrm{e}^{(1-\lambda)\varepsilon}\mathrm{e}^{\lambda\varepsilon}\Psi(x)$。由于所有量均为正，$\mathrm{e}^{\lambda\varepsilon}\Psi(x) < 1$；因此，$\Psi(x) < \mathrm{e}^{-\lambda\varepsilon} \Rightarrow x\in\mathcal{X}_H$。 □

具有 X不变随机化的看门狗机制是一种复杂度低且功能强大的方法，可以轻松应用于逐实例度量。然而，它会显著降低效用 [24] ，因为 X不变随机化将所有高风险符号统一进行混淆，以尽量减少隐私泄漏，但代价是数据分辨率降低。在第四节中，我们提出子集合并随机化，以提升看门狗机制的效用。

2）非对称最优随机响应（AORR）：ORR 已在 [27] 中被提出，作为隐私漏斗 [11] 的局部逐实例替代方法。它是在满足 ε-LIP 或 ε-LDP 隐私约束下，最优效用问题的解。对于 ALIP，我们提出非对称最优随机响应（AORR），其定义如下:

$$\begin{aligned} &\max_{P_{X|Y},P_Y} I(X;Y) \\ \text{s.t.}\quad &S - X - Y \\ &\mathrm{e}^{-\varepsilon_l} \le \Psi(y) \quad \text{and} \quad \Lambda(y) \le \mathrm{e}^{\varepsilon_u},\ \forall y\in\mathcal{Y}. \end{aligned} \tag{12}$$

该优化问题中的隐私约束构成一个闭、有界的凸多胞体 [27]。已有证明表明，该多胞体的顶点是能够使互信息最大化并满足隐私约束的可行候选解 [6], [27], [33]。然而，顶点数量会随多面体维度呈指数增长，对于 LDP 为 $|\mathcal{X}|(|\mathcal{X}|-1)$，对于 LIP 为 $(|\mathcal{X}|-1)$。这使得 ORR 在较大 $|\mathcal{X}|$ 下的计算十分繁琐。因此， [27] 提出了一些复杂度低于 ORR 的方法，以避免对较大规模 $\mathcal{X}$ 进行顶点枚举，但代价是效用降低。

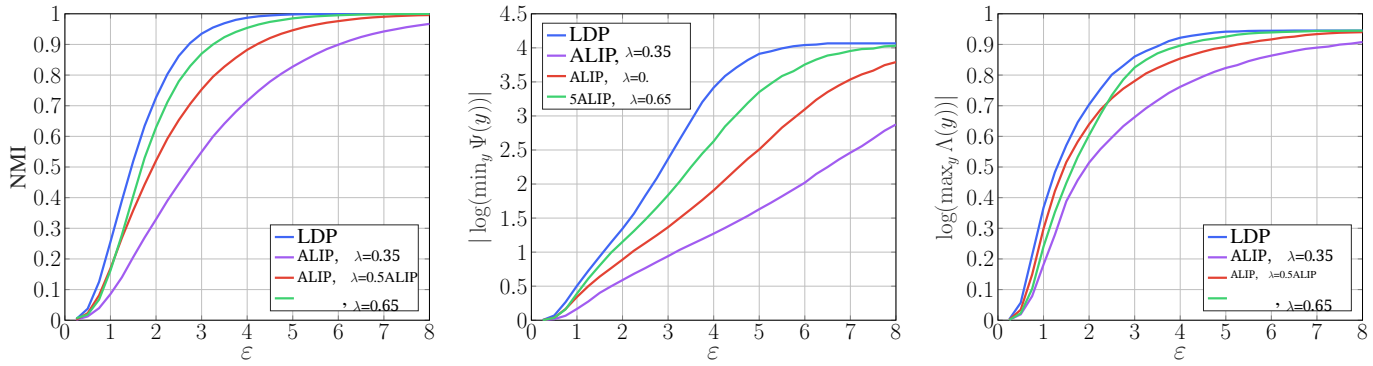
3) 数值结果：这里展示 ALIP 下 AORR 和看门狗机制的隐私泄漏与效用。对于效用，我们使用归一化互信息（NMI）

$$\text{NMI} = \frac{I(X;Y)}{H(X)} \in [0,1].$$

显然，当不进行随机化而直接发布 X 时，可获得最大可能效用，其中 $Y = X$ 和$I(X;Y) = H(X)$。因此， $I(X;Y) \le H(X)$，且 NMI ≤ 1。在数值模拟中，我们为看门狗机制随机生成了 10^3个分布，并为 AORR 生成了 100 个分布，其中 $|\mathcal{X}| = 17$ 和 $|\mathcal{S}| = 5$。随后，分别针对图2和图3中的看门狗机制与 AORR 机制，绘出了 NMI、$\log(\max_y \Lambda(y))$（最大提升泄漏）以及 $|\log(\min_y \Psi(y))|$（最小提升泄漏）的均值随 LDP 隐私预算 ε变化的情况。对于这两种机制， ε 在 0.25 到 8 之间变化；对于 $(\varepsilon_u,\varepsilon_l)$-ALIP，考虑了三种情况，其中 $\lambda\in\{0.35,0.5,0.65\}$、$\varepsilon_l = \lambda\varepsilon$，以及 $\varepsilon_u = (1-\lambda)\varepsilon$。

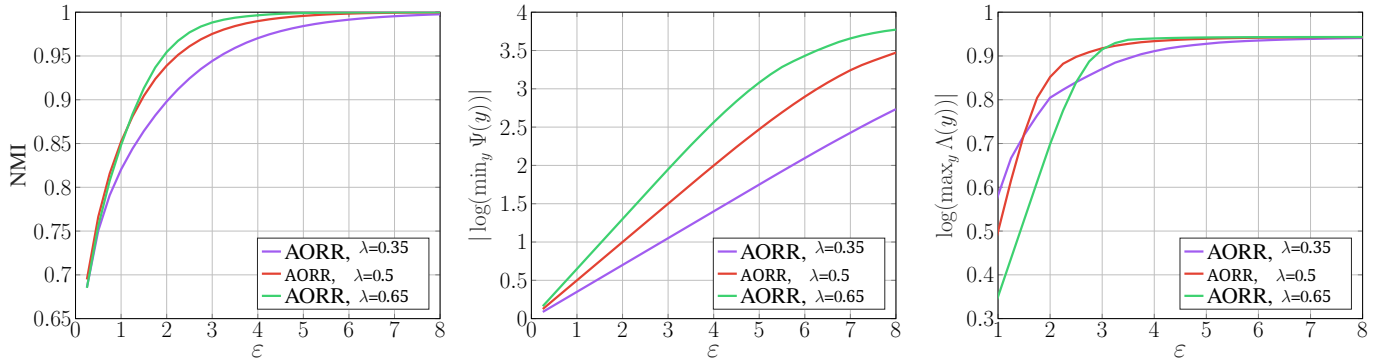
在图2中，我们观察到，对于所有 ε 和 λ 的取值，在看门狗机制中，LDP 的效用和泄漏均高于 ALIP，这证实了命题 2。图2a和图3a表明，对于 $\varepsilon > 1$，最小提升放宽 $\lambda = 0.65$ 提高了看门狗机制和 AORR 机制的效用。请注意，在这两幅图中， $\lambda = 0.5$ 指的是 $\frac{\varepsilon}{2}$-LIP。另一方面， $\lambda = 0.35$ 会导致效用降低。一般而言， $\lambda < 0.5$ 的任何取值都会降低效用，因为它对最小提升施加了严格限制，同时放宽了最大提升。由于最小提升的取值范围更广，达到这一严格限制会扩大集合 $\mathcal{X}_H$，并要求对更多符号进行随机化，从而降低效用。

另一个观察结果是，AORR 的效用显著高于看门狗机制。例如，当$\lambda = 0.5$ 和 $\varepsilon = 2$时，看门狗机制的效用为 0.52，而 AORR 的效用为 0.94。AORR 找到了最优效用；由于 PUT 的缘故，这必然会在满足隐私约束的前提下导致最高的泄漏。然而，看门狗机制是一种非最优方案，它通过最大限度地减少高风险符号的泄漏来提供强隐私保护



(a) 效用 (b) 最小提升泄漏 (c) 最大提升泄漏

图 2：在 ε-LDP 和 $(\varepsilon_l, \varepsilon_u)$-ALIP 下，采用完全合并随机化的看门狗机制的隐私-效用权衡，其中 $|\mathcal{X}| = 17$、$|\mathcal{S}| = 5$、$\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$、$\lambda \in \{0.35, 0.5, 0.65\}$、$\varepsilon_l = \lambda\varepsilon$ 和 $\varepsilon_u = (1-\lambda)\varepsilon$。



(a) 效用 (b) 最小提升泄漏 (c) 最大提升泄漏

图 3：AORR 的隐私-效用权衡，其中 $|\mathcal{X}| = 17$、$|\mathcal{S}| = 5$、$\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$、$\lambda \in \{0.35, 0.5, 0.65\}$、$\varepsilon_l = \lambda\varepsilon$ 和 $\varepsilon_u = (1-\lambda)\varepsilon$。

，但这会损害效用。为了解决看门狗机制的这一缺陷，我们将在下一节提出一种子集随机化方法。

IV. 看门狗机制中的子集合并

采用 X 不变随机化的看门狗机制是一种低复杂度方法，当隐私度量按符号定义时可以轻松应用。对于高风险符号，X 不变随机化是最优的隐私保护方式，可将 $\mathcal{X}_H$ 中的隐私泄漏降至最低，但必然导致最差的数据分辨率。因此，本节提出子集合并算法，通过对高风险符号的不相交子集进行随机化来提升数据分辨率，并增强看门狗机制中的效用。下文将说明，对 $\mathcal{X}_H$ 的不相交子集应用 X 不变随机化可以提高效用。

设 $\mathcal{G}_{\mathcal{X}_H} = \{\mathcal{X}_1, \mathcal{X}_2, \cdots \mathcal{X}_g\}$ 是 $\mathcal{X}_H$ 的一个划分，其中对于每个 $i \in [g]$、$\mathcal{X}_i \subseteq \mathcal{X}_H$：$\mathcal{X}_i \cap \mathcal{X}_j = \varnothing$、$i \neq j$，且 $\mathcal{X}_H = \cup_{i=1}^{g} \mathcal{X}_i$。我们通过 X-不变随机化 $\mathcal{R}_{\mathcal{Y}_i}(y)$ 对每个子集 $\mathcal{X}_i \in \mathcal{G}_{\mathcal{X}_H}$ 进行随机化，其中 $x \in \mathcal{X}_i$ 和 $y \in \mathcal{Y}_i$，且 $\sum_{y \in \mathcal{Y}_i} \mathcal{R}_{\mathcal{Y}_i}(y) = 1$。所得的 X 与 Y 之间的互信息为

$$I(X;Y) = H(X) - \sum_{i=1}^{g} \sum_{x \in \mathcal{X}_i} P_X(x) \log \frac{P(\mathcal{X}_i)}{P_X(x)}. \tag{13}$$

定义 4. 设有两个划分 $\mathcal{G}_{\mathcal{X}_H} = \{\mathcal{X}_1, \cdots, \mathcal{X}_g\}$ 和 $\mathcal{G}'_{\mathcal{X}_H} = \{\mathcal{X}'_1, \cdots, \mathcal{X}'_{g'}\}$。如果对于每个 $i \in [g]$、$\mathcal{X}_i = \cup_{j \in J_i} \mathcal{X}'_j$，其中 $J_i \subseteq [g']$，且 $P(\mathcal{X}_i) = \sum_{j \in J_i} P(\mathcal{X}'_j)$，则称[3] $\mathcal{G}'_{\mathcal{X}_H}$ 是 $\mathcal{G}_{\mathcal{X}_H}$ 的细化，或称 $\mathcal{G}_{\mathcal{X}_H}$ 是 $\mathcal{G}'_{\mathcal{X}_H}$ 的聚合。

如果 $\mathcal{G}'_{\mathcal{X}_H}$ 是 $\mathcal{G}_{\mathcal{X}_H}$ 的细化，那么 $I_{\mathcal{G}_{\mathcal{X}_H}}(X;Y) \leq I_{\mathcal{G}'_{\mathcal{X}_H}}(X;Y)$。

[3]这个定义受到 [34, 定义 10]的启发。

算法1：看门狗机制中的子集合并

1 输入： $\mathcal{X}$、ε_l、ε_u、P_{SX}.
2 输出： $\mathcal{G}_{\mathcal{X}_H}=\{\mathcal{X}_1,\mathcal{X}_2,\cdots\mathcal{X}_g\}$.
3 初始化：获取 $\{\mathcal{X}_L,\mathcal{X}_H\}$、 $\mathcal{X}_Q\leftarrow\mathcal{X}_H$ 和 $g=1$.
4 当 $(\Psi(\mathcal{X}_Q)<\mathrm{e}^{-\varepsilon_l}\quad or\quad \Lambda(\mathcal{X}_Q)>\mathrm{e}^{\varepsilon_u})$ 并且 $|\mathcal{X}_Q|>0$ 执行
5 $\quad\mathcal{X}_g=$ 取最大值 $\omega(x)$，以及 $\mathcal{X}_Q\leftarrow\mathcal{X}_Q\setminus\mathcal{X}_g$;
6 $\quad$当 $(\Psi(\mathcal{X}_g)<\mathrm{e}^{-\varepsilon_l}\quad or\quad \Lambda(\mathcal{X}_g)>\mathrm{e}^{\varepsilon_u})$ 并且 $|\mathcal{X}_Q|>0$ 执行
7 $\quad\quad x^*=\arg\min_{x\in\mathcal{X}_Q}\ \omega(\mathcal{X}_g\cup\{x\})$;
8 $\quad\quad\mathcal{X}_g\leftarrow\mathcal{X}_g\cup\{x^*\}$, 和 $\mathcal{X}_Q\leftarrow\mathcal{X}_Q\setminus\{x^*\}$;
9 $\quad$**end**
10 $\quad\mathcal{G}_{\mathcal{X}_Q}=\{\mathcal{X}_1,\mathcal{X}_2,\cdots,\mathcal{X}_g\}$, 和 $g\leftarrow g+1$;
11 结束
12 当 $(\Psi(\mathcal{X}_g)<\mathrm{e}^{-\varepsilon_l}\quad or\quad \Lambda(\mathcal{X}_g)>\mathrm{e}^{\varepsilon_u})\quad and\quad |\mathcal{G}_{\mathcal{X}_Q}|>1$ 执行
13 $\quad i^*=$ 取最小值 $_{1\le i<g}\ \omega(\mathcal{X}_g\cup\mathcal{X}_i)$, 并且 $\mathcal{X}_g\leftarrow\mathcal{X}_g\cup\mathcal{X}_{i^*}$;
14 $\quad$对于 $i^*+1\le j\le g$，将 $\mathcal{X}_j$ 的索引更新为 $\mathcal{X}_{j-1}$ 和 $g\leftarrow g-1$;
15 $\quad\mathcal{G}_{\mathcal{X}_Q}=\{\mathcal{X}_1,\mathcal{X}_2,\cdots,\mathcal{X}_g\}$;
16 结束

获得能够最大化效用并满足隐私约束的最优 $\mathcal{G}_{\mathcal{X}_H}$，需要在 $\mathcal{X}_H$的所有可能划分上求解组合优化问题，这十分繁琐。因此，我们在下文提出一种启发式方法。

A. 用于构造高风险符号细化子集的贪心算法

在算法1中，我们提出了一种自底向上算法，通过合并不相交子集中的高风险符号，对 $\mathcal{X}_H$ 进行划分。该算法基于针对每个 $x\in\mathcal{X}_H$的泄露风险度量：对于 ALIP，为 $\omega(x)=\Lambda(x)+\Psi(x)$；对于 LDP，为 $\omega(x)=\Gamma(x)$。对于 LIP，度量为 $\omega(x)=\max\{\log\ \Lambda(x)\ |\log\ \Psi(x)|\}$。该度量用于根据隐私风险等级对各子集排序。因此，为构造一个子集 $\mathcal{X}_i\subseteq\mathcal{X}_H$，算法1从风险最高的符号 $\mathcal{X}_i=\{\arg\max_{x\in\mathcal{X}_H}\omega(x)\}$ 开始（第5行）。随后，只要$\mathcal{X}_i$满足隐私约束，就将符号 x^* 与使 $\omega(\mathcal{X}_i\cup x^*)$最小的 $\mathcal{X}_i$ 合并（第7行）。在算法1中，对于第4、6和12行 while 循环的条件，我们使用了 ALIP 隐私约束。对于 LDP，隐私约束改为 $\Gamma(\mathcal{X}_Q)>\varepsilon$，并应用 $\omega(x)$进行 LDP。完成划分 $\mathcal{G}_{\mathcal{X}_H}$后，最后一个子集 $\mathcal{X}_g$ 可能不满足隐私约束。因此，我们会检查 $\mathcal{X}_g$ 的泄漏情况（第12行）；如果发生隐私泄露，则通过合并其他子集来聚合 $\mathcal{X}_g$，使 $\omega(\mathcal{X}_g)$最小（第13–14行），直至满足隐私约束。

B. 数值结果

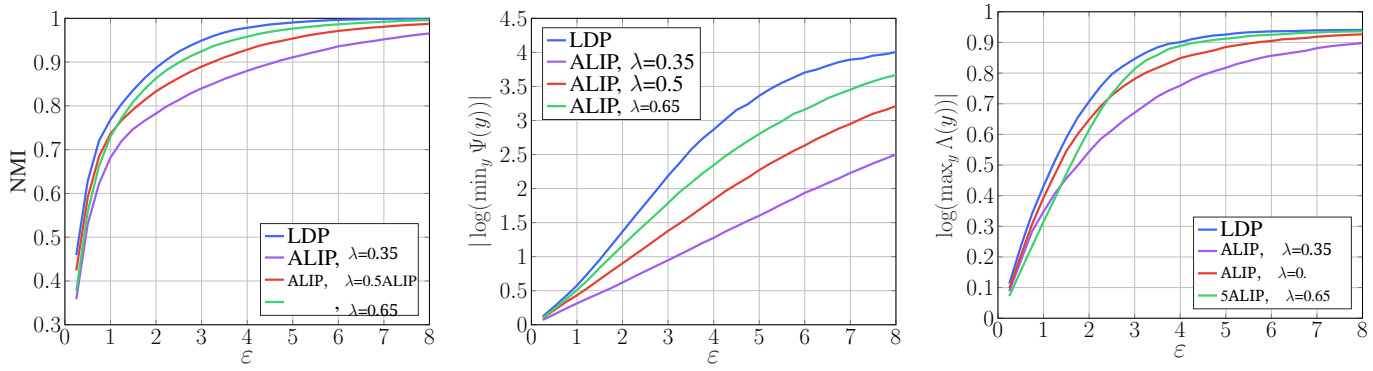
图 4 展示了在子集合并随机化下 ALIP 和 LDP 的 PUT，设置与 III-A3 节中的看门狗机制相同。与完全合并（图 2）相比，在相同隐私约束下，所有情形中的 LDP 和 ALIP 效用都显著提升。例如，考虑对称情形 $\lambda=0.5$when $\varepsilon=2$，并比较子集合并与完全合并的 PUT。图 4a 显示，子集合并的效用约为 0.83，而图 2a 中完全合并的效用为 0.52，效用几乎提升了 60%。此外，正如图 4b 和图 4c 所示，所有情况下都满足隐私约束。

V. 子集随机响应

上一节中，我们已展示子集合并能显著提升看门狗机制的效用。本节提出一种方法，以降低大型数据集上 AORR 的复杂度。我们对 $\mathcal{X}_H$ 的子集采用 AORR，以降低 AORR 处理大型集合时的复杂度，从而使随机响应适用于规模通常大一个数量级的 $\mathcal{X}$。

式 (12) 中的 AORR 优化问题等价于以下问题

$$\begin{aligned}&H(x)-\min_{P_{X|Y},P_Y}H(X|Y)\\ &\text{s.t.}\quad S-X-Y\\ &\qquad\mathrm{e}^{-\varepsilon_l}\le\Psi(y)\quad\text{and}\quad\Lambda(y)\le\mathrm{e}^{\varepsilon_u},\ \forall y\in\mathcal{Y}.\end{aligned}\tag{14}$$



(a) 效用　　(b) 最小提升泄漏　　(c) 最大提升泄漏

图 4：在 ε-LDP 和 $(\varepsilon_l, \varepsilon_u)$-ALIP 下，子集合并随机化的隐私-效用权衡，其中 $|\mathcal{X}| = 17$、$|\mathcal{S}| = 5$、$\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$、$\lambda \in \{0.35, 0.5, 0.65\}$、$\varepsilon_l = \lambda\varepsilon$ 和 $\varepsilon_u = (1-\lambda)\varepsilon$。

为降低式 (14) 的复杂度，我们将 $\mathcal{X}$ 划分为 $\mathcal{X}_L$ 和 $\mathcal{X}_H$，类似于看门狗机制，并从 $\mathcal{X}_H$中构造划分$\mathcal{G}_{\mathcal{X}_H} = \{\mathcal{X}_1, \mathcal{X}_2, \cdots \mathcal{X}_g\}$。我们分别使用随机化对 $(\mathsf{Q}_i, \mathsf{q}_i)$ 对每个子集 $\mathcal{X}_i \in \mathcal{G}_{\mathcal{X}_H}$、$i \in [g]$进行随机化，其中 Q_i是 $\mathbb{R}^{|\mathcal{X}_i|\times|\mathcal{Y}_i|}$中的矩阵，$\mathsf{q}_i$是 $\mathbb{R}^{|\mathcal{Y}_i|}$中的向量。$\mathsf{Q}_i$和 q_i的元素分别由 $\mathsf{Q}_i(x|y) = \Pr[X = x|Y = y]$、$x \in \mathcal{X}_i$、$y \in \mathcal{Y}_i$ 以及 $\mathsf{q}_i(y) = \Pr[Y = y]$、$y \in \mathcal{Y}_i$给出。对于每个 $y \in \mathcal{Y}_i$，有 $\sum_{x\in\mathcal{X}_i} \mathsf{Q}_i(x|y) = 1$。因此，$H(X|Y) = \sum_{i\in[g]} H_i(X|Y)$，其中 $H_i(X|Y) = -\sum_{y\in\mathcal{Y}_i} \mathsf{q}_i(y) \sum_{x\in\mathcal{X}_i} \mathsf{Q}_i(x|y) \log \mathsf{Q}_i(x|y)$。该设置将式 (14) 转化为针对每个子集 $\mathcal{X}_i \in \mathcal{G}_{\mathcal{X}_H}$、$i \in [g]$ 的 g 个优化问题，如下所示：

$$
\begin{aligned}
&\min_{\mathsf{Q}_i, \mathsf{q}_i} && H_i(X|Y) && && (15)\\
\text{s.t.}\quad & 0 \le \mathsf{q}_i(y), && && \forall y \in \mathcal{Y}_i, && (16)\\
& 0 \le \mathsf{Q}_i(x|y), && && \forall x \in \mathcal{X}_i, \forall y \in \mathcal{Y}_i, && (17)\\
& \sum_{x\in\mathcal{X}_i} \mathbf{Q}_i(x|y) = 1, && && \forall y \in \mathcal{Y}_i, && (18)\\
& \sum_{y\in\mathcal{Y}_i} \mathsf{Q}_i(x|y)\mathsf{q}_i(y) = P_X(x), && && x \in \mathcal{X}_i, && (19)\\
& \mathrm{e}^{-\varepsilon_l} P_S(s) \le \sum_{x\in\mathcal{X}_i} P_{S|X}(s|x)\mathsf{Q}_i(x|y) \le \mathrm{e}^{\varepsilon_u} P_S(s), && && \forall s \in \mathcal{S}, y \in \mathcal{Y}_i. && (20)
\end{aligned}
$$

随机化矩阵 Q_i, $i \in [g]$ 的列可以表示为凸有界多面体Π_i的成员，该多面体由以下约束给出

$$
\Pi_i = \left\{ \begin{array}{l} \mathbf{v} \in \mathbb{R}^{|\mathcal{X}_i|}: \\ 0 \le v_k, \forall k \in [|\mathcal{X}_i|], \\ \sum_{k=1}^{|\mathcal{X}_i|} v_k = 1, \\ \mathrm{e}^{-\varepsilon_l} P_S(s) \le \sum_{x\in\mathcal{X}_i} P_{S|X}(s|x) v_k \le \mathrm{e}^{\varepsilon_u} P_S(s), \forall s \in \mathcal{S}, k \in [|\mathcal{X}_i|] \end{array} \right\}. \tag{21}
$$

对于每个 $\mathcal{X}_i \in \mathcal{G}_{\mathcal{X}_H}$, $i \in [g]$，令 $\mathcal{V}_i = \{\mathbf{v}_1^i \cdots, \mathbf{v}_M^i\}$ 为式 (21) 中 Π_i 的顶点，$\mathrm{H}\left(\mathbf{v}_k^i\right)$ 为每个 $\mathbf{v}_k^i$ 的熵（对于 $k \in [M]$），$\boldsymbol{P}_{\boldsymbol{X}}^{\boldsymbol{i}}$ 为 $x \in \mathcal{X}_i$ 的概率向量，而 $\boldsymbol{\beta}^i$ 为以下优化问题的解

$$
\begin{aligned}
&\min_{\boldsymbol{\beta}^i \in \mathbb{R}^M} \sum_{k=1}^{M} \mathrm{H}\left(\mathbf{v}_k^i\right) \beta_k^i, \\
\text{s.t.}\quad & \beta_k^i \ge 0, \quad \forall k \in [M], \\
& \sum_{k=1}^{M} \mathbf{v}_k^i \beta_k^i = \boldsymbol{P}_{\boldsymbol{X}}^{\boldsymbol{i}}.
\end{aligned} \tag{22}
$$

然后，$\mathcal{Y}_i$ 和 $(\mathsf{Q}_i, \mathsf{q}_i)$ 定义如下：

$$
\mathcal{Y}_i = \{y : \beta_y^i \ne 0\}; \tag{23}
$$

$$
\mathbf{q}_i(y) = \beta_y^i \quad \text{and} \quad \mathbf{Q}_i(.|y) = \mathbf{v}_y^i, \quad y \in \mathcal{Y}_i. \tag{24}
$$

$(\varepsilon_l, \varepsilon_u)$-ALIP 协议 $\mathcal{M}$：$\mathcal{X} \to \mathcal{Y}$ 由以下 $(P_{X|Y}, P_Y)$ 对给出：

$$P_{X|Y} = \begin{cases} \mathbf{1}_{\{x=y\}}, & x, y \in \mathcal{X}_L = \mathcal{Y}_L, \\ \mathbf{Q}_i(x|y), & x \in \mathcal{X}_i, y \in \mathcal{Y}_i, i \in [g], \\ 0, & \text{otherwise;} \end{cases} \tag{25}$$

$$P_Y = \begin{cases} P_X(y), & y \in \mathcal{Y}_L, \\ \mathbf{q}_i(y), & y \in \mathcal{Y}_i, i \in [g]. \end{cases} \tag{26}$$

算法 2：子集随机响应

1 输入：$\mathcal{X}, \varepsilon_l, \varepsilon_u, P_{SX}$。
2 输出：$\mathcal{O}_{\mathcal{X}_H} = \{\mathcal{X}'_1, \mathcal{X}'_2, \cdots \mathcal{X}'_{g'}\}$, $P_{X|Y}$和 P_Y。
3 初始化：通过算法1获取 $\mathcal{G}_{\mathcal{X}_H} = \{\mathcal{X}_1, \mathcal{X}_2, \cdots \mathcal{X}_g\}$ 和 $g' = 1$。
4 当 $|\mathcal{G}_{\mathcal{X}_H}| > 0$ 时
5 $\mathcal{X}'_{g'} = \mathcal{X}_1$，在(21)中找到 $\Pi_{g'}$，并且 $\mathcal{G}_{\mathcal{X}_H} \leftarrow \mathcal{G}_{\mathcal{X}_H} \setminus \mathcal{X}_1$;
6 更新 $\mathcal{G}_{\mathcal{X}_H}$ 中的子集索引，使得 $\mathcal{X}_{i-1} \leftarrow \mathcal{X}_i$ 适用于 $2 \le i \le g$ 和 $g \leftarrow g-1$;
7 当 $\Pi_{g'} = \varnothing$ 且（$|\mathcal{G}_{\mathcal{X}_H}| > 0$ 或 $|\mathcal{O}_{\mathcal{X}_H}| > 0$）时执行
8 如果 $|\mathcal{G}_{\mathcal{X}_H}| > 0$，则
9 $\mathcal{X}'_{g'} = \mathcal{X}'_{g'} \cup \mathcal{X}_1$，在 (21) 中求得 $\Pi_{g'}$，并求得 $\mathcal{G}_{\mathcal{X}_H} \leftarrow \mathcal{G}_{\mathcal{X}_H} \setminus \mathcal{X}_1$;
10 更新 $\mathcal{G}_{\mathcal{X}_H}$ 中的子集索引，使得 $\mathcal{X}_{i-1} \leftarrow \mathcal{X}_i$ 适用于 $2 \le i \le g$ 和 $g \leftarrow g-1$;
11 **else**
12 $\mathcal{X}'_{g'} = \mathcal{X}'_{g'} \cup \mathcal{X}'_{g'-1}$、 $g' \leftarrow g'-1$，并在 (21) 中求得 $\Pi_{g'}$;
13 **end**
14 **end**
15 设定 $\mathcal{O}_{\mathcal{X}_H} = \{\mathcal{X}'_1, \mathcal{X}'_2, \cdots \mathcal{X}'_{g'}\}$ 和 $g' \leftarrow g'+1$;
16 结束
17 如果 $|\mathcal{O}_{\mathcal{X}_H}| = 1$ 和 $\Pi_1 = \varnothing$，则
18 对 $\mathcal{G}_{\mathcal{X}_H}$ 应用子集合并机制。
19 否则
20 对 $i \leftarrow 1$ 到 g' 执行
21 求解 $\mathcal{X}$中的优化问题（22） i' 并获得 $\boldsymbol{\beta_i}$、Q_i和q_i;
22 **end**
23 获得（25）中的 $P_{X|Y}$ 和（26）中的 P_Y。
24 结束

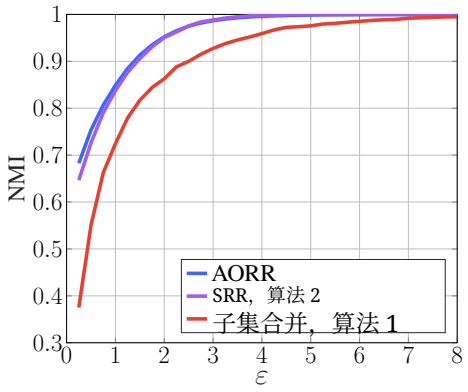
A. 子集随机响应算法

我们提出算法 2，以对 $\mathcal{X}_H$的子集实施 AORR，并将其称为子集随机响应（SRR）。在该算法中，首先通过算法1获得 $\mathcal{X}_H$的划分 $\mathcal{G}_{\mathcal{X}_H} = \{\mathcal{X}_1, \mathcal{X}_2, \cdots \mathcal{X}_g\}$。然后，我们为每个子集 $\mathcal{X}'_i \in \mathcal{G}_{\mathcal{X}_H}$寻找最优随机响应（第5行）。通过获得所有子集的最优随机响应，我们为每个子集 $\mathcal{X}'_i$得到一对（Q_i，q_i），并据此根据（25）和（26）得到 $P_{X|Y}$和 P_Y（第20—23行）。第7—14行中的 while 循环用于处理以下特殊情况：对于某个子集 $\mathcal{X}'_i$，式（21）中的多面体为空。这种情况可能发生在严格的隐私条件下，此时隐私预算非常小。由于我们降低了式（14）中原始多面体的维度，因此在某些情况下不存在可行随机响应的可能性增加了。因此，在这种情况下，我们将 $\mathcal{G}_{\mathcal{X}_H}$ 中的其他子集并入（第9行），或将 $\mathcal{O}_{\mathcal{X}_H}$ 并入（第12行），直到得到一个非空多面体。第17—18行中的 if 条件用于以下情况：将所有子集合并后仍不存在可行多面体。每当发生这种情况时，我们便应用子集合并机制。

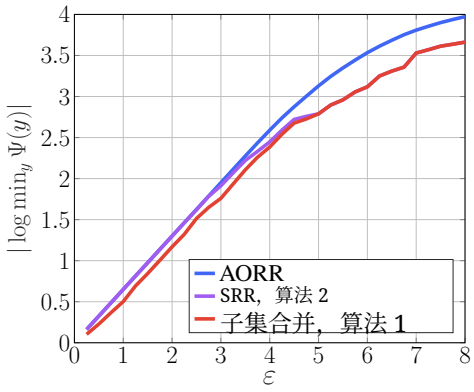
AORR 中的多胞体顶点数量为 $n \sim O(\exp(|\mathcal{X}|-1))$，时间复杂度为 $O(n)$。随着 $|\mathcal{X}|$ 的增加，AORR 的复杂度在 $|\mathcal{X}|-1$ 中呈指数增长。在 SRR 中，对于每个 $\mathcal{X}_i \in \mathcal{G}_{\mathcal{X}_H}$、$i \in [g]$，顶点数量为 $n_i \sim O(\exp(|\mathcal{X}_i|-1))$，SRR 的复杂度为 $O(\max_i n_i)$。因此，SRR 的复杂度随着最大子集大小的增加而增加，而该大小可能远低于 AORR 中的对应值。

B. 数值结果

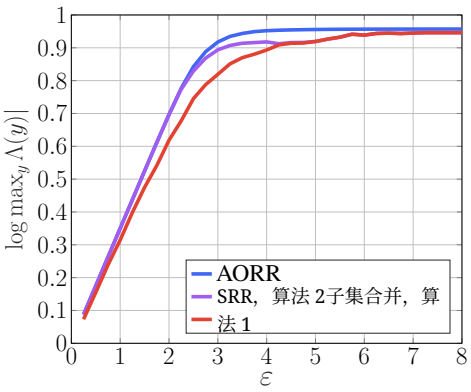
这里，我们比较算法 2 中 AORR 与 SRR 的 PUT，以及算法1 中的子集合并。图5展示了100个随机生成的分布的效用、泄漏和时间复杂度的均值，其中 $\lambda = 0.65$，且仿真设置与 III-A3 节中的相同。



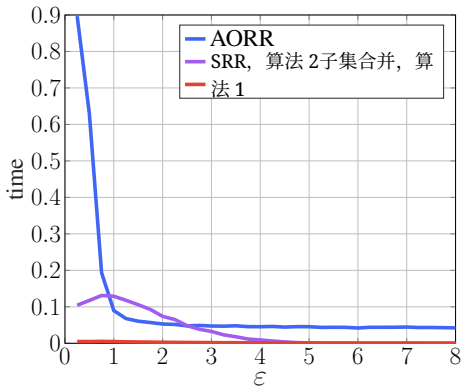
(a) 效用



(b) 最小提升泄漏

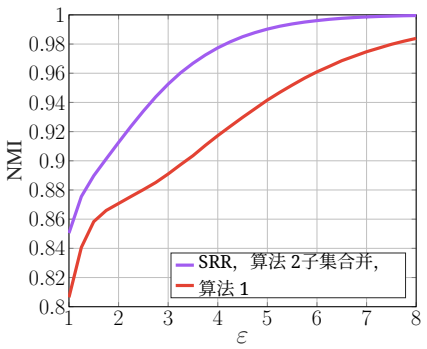


(c) 最大提升泄漏

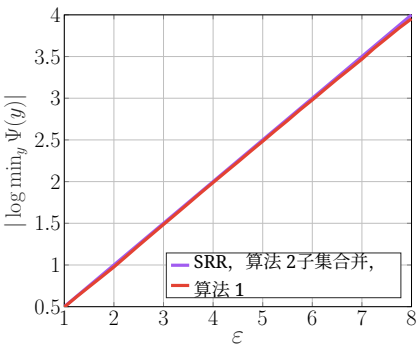


(d) 时间复杂度

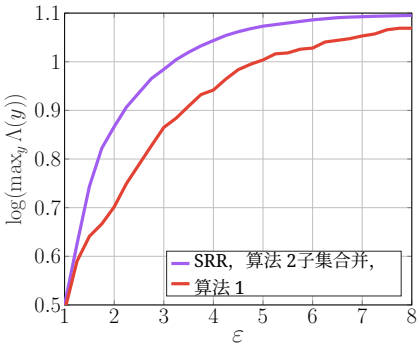
图 5：AORR、SRR 与子集合并在隐私-效用权衡和时间复杂度方面的比较，其中 $|\mathcal{X}| = 17$、$|\mathcal{S}| = 5$、$\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$、$\lambda = 0.65$、$\varepsilon_l = \lambda\varepsilon_{\text{LDP}}$ 和 $\varepsilon_u = (1-\lambda)\varepsilon_{\text{LDP}}$。



(a) 效用



(b) 最小提升泄漏



(c) 最大提升泄漏

图 6：SRR 与子集合并在隐私-效用权衡和时间复杂度方面的比较，其中 $|\mathcal{X}| = 200$、$|\mathcal{S}| = 15$、$\varepsilon_{\text{LDP}} \in \{1, 1.25, 1.5, 1.75, \cdots, 8\}$ 和 $\varepsilon_l = \varepsilon_u = \frac{\varepsilon_{\text{LDP}}}{2}$。

图5a至图5c表明，与子集合并相比，SRR能够获得更好的效用，但泄漏更高，并且其 PUT 与 AORR 非常接近。图5d展示了每种机制的处理时间，由此我们观察到，AORR 和 SRR 的复杂度远高于子集合并。在严格隐私约束（$\varepsilon < 1$）以及 $\varepsilon > 2.5$ 的情况下，运行 SRR 的复杂度低于 AORR。尽管在某些隐私预算下 SRR 的复杂度更高（$1 \le \varepsilon \le 2.5$），但它在高维系统中具有优势。图6展示了 SRR 与子集合并之间的 PUT 比较，其中 $|\mathcal{X}| = 200$、$|\mathcal{S}| = 15$、$\varepsilon \in \{1, 1.25, \cdots, 8\}$ 和 $\lambda = 0.5$。该实验表明，SRR 和子集合并都适用于大型数据集。显然，SRR 提供了更好的效用（图6a）和更高的泄漏（图6b和图6c），但仍低于

给定预算 ε_l 和 ε_u。

VI. 基于提升和提升逆的度量

本节将介绍近期提出的一些隐私度量，它们用于量化敏感特征的后验信念与先验信念之间的差异，包括 ℓ_1-范数 [28], 强 χ^2-隐私准则 [29], 和 α-提升 [30]。这些度量被提出作为相应平均度量的更强版本，后者分别为全变差距离 [31],χ^2-散度 [35], 和 Sibson互信息 [15], 。我们将它们称为基于提升的度量，并在下文中给出定义。

定义 5. 对于每个 $y \in \mathcal{Y}$，基于提升的隐私度量定义如下：

- 所述 ℓ_1-提升定义为

$$\Lambda_{\ell_1}(y) \triangleq \sum_{s\in\mathcal{S}} P_S(s)|l(s,y)-1|, \tag{27}$$

那么，全变差距离为

$$T(S;Y) = \frac{1}{2}\mathbb{E}_Y[\Lambda_{\ell_1}(Y)].$$

- χ^2提升定义为

$$\Lambda_{\chi^2}(y) \triangleq \sum_{s\in\mathcal{S}} P_S(s)\big(l(s,y)-1\big)^2, \tag{28}$$

则 χ^2-散度为

$$\chi^2(S;Y) = \mathbb{E}_Y[\Lambda_{\chi^2}(Y)].$$

- α提升定义为

$$\Lambda_\alpha^S(y) \triangleq \left(\sum_{s\in\mathcal{S}} P_S(s) l(s,y)^\alpha\right)^{1/\alpha}, \tag{29}$$

则 Sibson互信息为

$$I_\alpha^S(S;Y) = \frac{\alpha}{\alpha-1}\log \mathbb{E}_Y[\Lambda_\alpha^S(Y)].$$

这里，我们揭示它们与 ALIP 的关系。

命题 3. 若满足 $(\varepsilon_b, \varepsilon_u)$-ALIP，则，

1) $\max\limits_{y\in\mathcal{Y}} \Lambda_{\ell_1}(y) \le \mathrm{e}^{\varepsilon_u} - 1$,

2) $\max\limits_{y\in\mathcal{Y}} \Lambda_{\chi^2}(y) \le (\mathrm{e}^{\varepsilon_u} - 1)^2$,

3) $\max\limits_{y\in\mathcal{Y}} \Lambda_\alpha^S(y) \le \mathrm{e}^{\varepsilon_u}$.

证明见附录 C。

命题4. 令 $s_y = \operatorname{argmax}\limits_{s\in\mathcal{S}}[l(s,y)]$ 和 $\bar{y} = \arg\max_{y\in\mathcal{Y}} \Lambda(y)$，则，

1) If $\max\limits_{y\in\mathcal{Y}} \Lambda_{\ell_1}(y) \le \varepsilon \Rightarrow \max\limits_{y\in\mathcal{Y}} \Lambda(y) \le \varepsilon/P_S(s_{\bar{y}}) + 1$,

2) If $\max\limits_{y\in\mathcal{Y}} \Lambda_{\chi^2}(y) \le \varepsilon \Rightarrow \max\limits_{y\in\mathcal{Y}} \Lambda(y) \le \sqrt{\varepsilon/P_S(s_{\bar{y}})} + 1$,

3) If $\max\limits_{y\in\mathcal{Y}} \Lambda_\alpha^S(y) \le \varepsilon \Rightarrow \max\limits_{y\in\mathcal{Y}} \Lambda(y) \le \varepsilon/P_S(s_{\bar{y}})^{\frac{1}{\alpha}}$.

证明。证明见附录D。 □

命题 3 表明，与相应的平均泄漏类似，基于提升的度量均受最大提升界的上界约束。命题4指出，如果我们对基于提升的度量进行界定，它们只能限制最大提升泄漏。因此，如果仅应用基于提升的度量来保护隐私，例如以往的工作 [28]–[30], ，可能会导致最小提升上的严重泄漏。因此，下面我们提出提升逆度量，以界定最小提升泄漏。

A. 提升逆度量

在命题3和命题4中，我们已经证明，基于提升的度量只能界定最大提升。在本小节中，我们提出提升逆度量，以限制最小提升泄漏，$\min_{y\in\mathcal{Y}}\Psi(y)=\min_{y\in\mathcal{Y}}[\min_{s\in\mathcal{S}} l(s,y)]$。

定义6. 对于式 (27) 至 (29) 中基于提升的度量，我们将 $l(s,y)$ 替换为 $l\ \frac{1}{s\ \cancel{(,y)}}$，并将所得量称为提升逆度量。

- ℓ_1提升逆度量定义为

$$\Psi_{\ell_1}(y)=\sum_{s\in\mathcal{S}}P_S(s)\left|\frac{1}{\ell(s,y)}-1\right|. \tag{30}$$

- χ^2提升逆度量定义为

$$\Psi_{\chi^2}(y)\triangleq\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{\ell(s,y)}-1\right)^2. \tag{31}$$

- α提升逆度量定义为

$$\Psi_\alpha^S(y)\triangleq\left(\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{\ell(s,y)}\right)^\alpha\right)^{1/\alpha}. \tag{32}$$

在以下命题中，我们将展示 $(\varepsilon_l,\varepsilon_u)$-ALIP 之间的关系。

命题5. 若实现了 $(\varepsilon_l,\varepsilon_u)$-ALIP，则有

1) $\max_{y\in\mathcal{Y}}\Psi_{\ell_1}(y)\le e^{\varepsilon_l}-1$,

2) $\max_{y\in\mathcal{Y}}\Psi_{\chi^2}(y)\le(e^{\varepsilon_l}-1)$

^{2},3) $\max_{y\in\mathcal{Y}}\Psi_\alpha^S(y)\le e^{\varepsilon_l}$.

证明. 证明见附录 E。 □

命题6. 令 $s_y=\operatorname{argmin}\ l(s,y)$ 且 $\underline{y}=\arg\min[\Psi(y)]$, 则, s y

1) If $\max_{y\in\mathcal{Y}}\Psi_{\ell_1}(y)\le\varepsilon\Rightarrow\min_{y\in\mathcal{Y}}\Psi(y)\ge\dfrac{P_S(s_{\underline{y}})}{\varepsilon+P_S(s_{\underline{y}})}$,

2) If $\max_{y\in\mathcal{Y}}\Psi_{\chi^2}(y)\le\varepsilon\Rightarrow\min_{y\in\mathcal{Y}}\Psi(y)\ge\dfrac{\sqrt{P_S(s_{\underline{y}})}}{\sqrt{\varepsilon}+\sqrt{P_S(s_{\underline{y}})}}$,

3) If $\max_{y\in\mathcal{Y}}\Psi_\alpha^S(y)\le\varepsilon\Rightarrow\min_{y\in\mathcal{Y}}\Psi(y)\ge\varepsilon^{-1}P_S(s_{\underline{y}})^{\frac{1}{\alpha}}$.

证明. 证明见附录 F。 □

命题5和命题6表明，上述提升逆度量与最小提升相关，对其进行界定可以限制最小提升泄漏。由于基于提升和提升逆的度量通过对敏感特征取平均的提升函数来量化隐私泄漏，因此可视为比最小提升和最大提升更宽松的度量。

B. PUT与数值结果

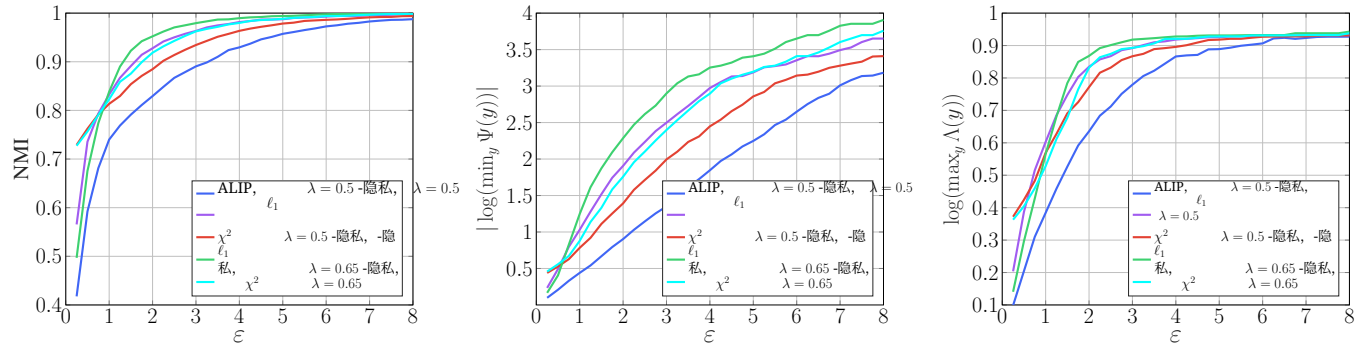
针对以互信息作为效用度量的 ℓ_1-提升和 χ^2-提升隐私，分别已有研究提出了最优随机化方法[28] 和 [29], 。请注意，由于这些度量的隐私约束并非凸约束，因此ORR不适用于这些度量。不过，在此我们采用看门狗机制与子集合并随机化，研究基于提升和提升逆的度量对应的PUT。此应用表明，看门狗机制结合 X-不变随机化是一种低复杂度方法，可应用于上述所有度量。此外，我们的子集合并算法显著提升了效用，其结果可与最优解相媲美。

为了将基于提升和提升逆的度量应用于子集合并算法，我们将式（6）和算法1中的 Λ（y）与 Ψ（y）分别替换为定义5和定义6中相应的基于提升和提升逆的度量。例如，对于 α-提升， $\mathcal{X}_L$ 和 $\mathcal{X}_H$可表示为

$$\mathcal{X}_L\triangleq\{x\in\mathcal{X}:\Psi_\alpha^S(x)\le e^{\varepsilon_l}\quad and\quad\Lambda_\alpha^S(x)\le e^{\varepsilon_u}\}\quad and\quad\mathcal{X}_H=\mathcal{X}\setminus\mathcal{X}_L. \tag{33}$$

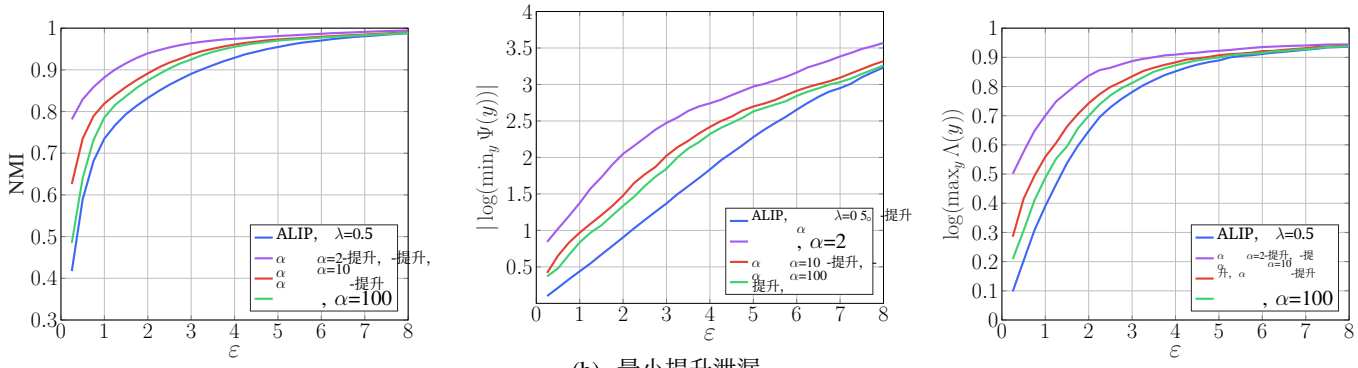
算法1中的隐私风险度量也由 $\omega(x)=\Psi_\alpha^S(x)+\Lambda_\alpha^S(x)$ 给出。我们将基于提升和提升逆的隐私的 PUT 与 $(\varepsilon_l,\varepsilon_u)$-ALIP 进行比较，其中基于提升和提升逆的度量界定如下：

- ℓ_1-隐私：$\Lambda_{\ell_1}(y)\le e^{\varepsilon_u}-1$ 和 $\Psi_{\ell_1}(y)\le e^{\varepsilon_l}-1,\qquad\forall y\in\mathcal{Y}$.



(a) 效用 (b) 最小提升泄漏 (c) 最大提升泄漏

图 7：ALIP、 ℓ_1-隐私和 χ^2-隐私之间的隐私-效用权衡比较，其中 $|\mathcal{X}| = 17$, $|\mathcal{S}| = 5$, $\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$, $\lambda \in \{0.5, 0.65\}$, $\varepsilon_l = \lambda\varepsilon$ 以及 $\varepsilon_u = (1-\lambda)\varepsilon$。



(a) 效用 (b) 最小提升泄漏 (c) 最大提升泄漏

图 8：ALIP 与 α-提升隐私之间的隐私-效用权衡比较，其中 $|\mathcal{X}| = 17$, $|\mathcal{S}| = 5$, $\varepsilon_{\text{LDP}} \in \{0.25, 0.5, 0.75, \cdots, 8\}$, $\varepsilon_l = \varepsilon_u = \frac{\varepsilon_{\text{LDP}}}{2}$ 和 $\alpha \in \{2, 10, 100\}$。

- χ^2-privacy: $\Lambda_{\chi^2}(y) \le (\mathrm{e}^{\varepsilon_u} - 1)^2$ and $\Psi_{\chi^2}(y) \le (\mathrm{e}^{\varepsilon_l} - 1)^2$, $\forall y \in \mathcal{Y}$.
- α-lift-privacy: $\Lambda^S_\alpha(y) \le \mathrm{e}^{\varepsilon_u}$ and $\Psi^S_\alpha(y) \le \mathrm{e}^{\varepsilon_l}$, $\forall y \in \mathcal{Y}$.

我们采用了 III-A3 节仿真设置中的子集合并机制。图 7 展示了在 $\lambda = \{0.5, 0.65\}$ 的 $\lambda = 0.5$、 ℓ_1 和 χ^2 隐私下，ALIP 的 PUT。当 $\lambda = 0.5$、 ℓ_1 和 χ^2 隐私相较于 ALIP 在 ε 的所有取值下都能带来更高的效用时，这是因为基于提升和提升逆的度量是最大提升和最小提升的松弛。为观察非对称场景的影响，我们绘制了 $\lambda = 0.65$ 的 ℓ_1 和 χ^2 隐私。从图 7a 可以观察到，提升逆松弛（$\lambda = 0.65$）显著提高了 $\varepsilon > 1$ 的效用，但降低了 $\varepsilon < 1$ 的效用。其原因在于，当 $\varepsilon < 1$ 时，非对称场景中的提升逆隐私约束较为严格，需要在每个子集中合并更多符号，从而导致子集变大并造成效用下降。

图 8 展示了 α-提升隐私与 ALIP 在 $\alpha \in \{2, 10, 100\}$ 下的比较。α-提升隐私具有可调性：当 $\alpha = \infty$ 时，它等同于 ALIP；当 $\alpha < \infty$ 时，则会产生一种放宽情形。我们从图 8 中观察到这种可调性，其中 $\alpha = 2$ 具有最高效用。此外，随着 α 增加， α- 提升隐私的 PUT 会越来越接近 ALIP。

VII. 结论

本文研究了提升，即数据集中有关敏感特征的后验信念与先验信念之间的似然比。我们阐明了从数据隐私角度看，最小提升和最大提升之间的区别。我们提出了 ALIP，作为 LIP 的一种广义形式，以实现一种与提升不对称性更相容的隐私概念。ALIP 能够提高看门狗机制和 ORR 机制这两种实现基于提升的隐私的主要方法的效用。我们提出了两种子集随机化方法，以提高看门狗机制的效用，并降低大型数据集的 ORR 复杂度。我们还研究了现有的基于提升的度量，发现它们可能导致最小提升发生严重泄漏。因此，我们提出了提升逆度量，以限制最小提升泄漏。最后，我们应用看门狗机制研究了基于提升和提升逆的度量的 PUT。未来的研究可以探讨最小提升和最大提升的适用操作含义。

子集随机化可用于降低其他隐私机制的复杂度并提高其效用。此外，针对 α-提升的最优随机化尚属未知，也值得进一步研究。

附录 A

1) 在 LDP 中，对于所有 $y \in \mathcal{Y}$，我们有

$$\Gamma(y) = \sup_{s,s' \in \mathcal{S}} \frac{P_{Y|S}(y|s)}{P_{Y|S}(y|s')} = \frac{\max_{s\in\mathcal{S}} P_{Y|S}(y|s)}{\min_{s\in\mathcal{S}} P_{Y|S}(y|s)} = \frac{\max_{s\in\mathcal{S}} P_{Y|S}(y|s)/P_Y(y)}{\min_{s\in\mathcal{S}} P_{Y|S}(y|s)/P_Y(y)} = \frac{\Lambda(y)}{\Psi(y)} \leq \frac{\mathrm{e}^{\varepsilon_u}}{\mathrm{e}^{-\varepsilon_l}} = \mathrm{e}^{\varepsilon_l+\varepsilon_u}.$$

2) 对于互信息，我们有

$$I(S;Y) = \mathbb{E}_{P_{SY}}[i(S,Y)] \leq \mathbb{E}_{P_{SY}}[\varepsilon_u] = \varepsilon_u.$$

3) • 对于全变差距离，我们有

$$\begin{aligned} T(S;Y) &= \frac{1}{2}\sum_{y\in\mathcal{Y}} P_Y(y) \sum_{s\in\mathcal{S}} P_S(s)|l(s,y)-1| \leq \frac{1}{2}\sum_{y\in\mathcal{Y}} P_Y(y) \sum_{s\in\mathcal{S}} P_S(s)|\Lambda(y)-1| \\ &= \frac{1}{2}\sum_{y\in\mathcal{Y}} P_Y(y)|\Lambda(y)-1| \leq \frac{1}{2}\sum_{y\in\mathcal{Y}} P_Y(y)|\mathrm{e}^{\varepsilon_u}-1| = \frac{1}{2}(\mathrm{e}^{\varepsilon_u}-1). \end{aligned}$$

• 对于 χ^2-散度，我们有

$$\begin{aligned} \chi^2(S;Y) &= \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{s\in\mathcal{S}} P_S(s)\big(l(s,y)-1\big)^2 \leq \sum_{y\in\mathcal{Y}} P_Y(y) \sum_{s\in\mathcal{S}} P_S(s)\big(\Lambda(y)-1\big)^2 \\ &= \sum_{y\in\mathcal{Y}} P_Y(y)\big(\Lambda(y)-1\big)^2 \leq \sum_{y\in\mathcal{Y}} P_Y(y)\big(\mathrm{e}^{\varepsilon_u}-1\big)^2 = (\mathrm{e}^{\varepsilon_u}-1)^2. \end{aligned}$$

4) • 对于 Sibson互信息，我们有

$$\begin{aligned} I_\alpha^S(S;Y) &= \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_S(s) l(s,y)^\alpha\right)^{1/\alpha} \\ &\leq \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_S(s) \Lambda(y)^\alpha\right)^{1/\alpha} \\ &\leq \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_S(s) \mathrm{e}^{\varepsilon_u\alpha}\right)^{1/\alpha} = \frac{\varepsilon_u\alpha}{\alpha-1}. \end{aligned}$$

• 对于 Arimoto互信息，我们有

$$\begin{aligned} I_\alpha^A(S;Y) &= \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_{S_\alpha}(s) l(s,y)^\alpha\right)^{1/\alpha} \\ &\leq \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_{S_\alpha}(s) \Lambda(y)^\alpha\right)^{1/\alpha} \\ &\leq \frac{\alpha}{\alpha-1}\log \sum_{y\in\mathcal{Y}} P_Y(y) \left(\sum_{s\in\mathcal{S}} P_{S_\alpha}(s) \mathrm{e}^{\varepsilon_u\alpha}\right)^{1/\alpha} = \frac{\varepsilon_u\alpha}{\alpha-1}, \end{aligned}$$

其中 $P_{S_\alpha}(s) = \frac{P_S(s)^\alpha}{\sum_{s\in\mathcal{S}} P_S(s)^\alpha}$.

APPENDIX B

在此，我们证明，对于 LDP， X-不变随机化可使 $\mathcal{X}_H$ 中的隐私泄漏最小化。

命题 7. 随机化 $r(y|x)$， $x, y, \in \mathcal{X}_H$ 能够满足 $(\varepsilon, \mathcal{X}_H)$-LDP，当且仅当：

$$\Gamma_{LDP}(\mathcal{X}_H) = \frac{\max_{s\in\mathcal{S}} P(\mathcal{X}_H|s)}{\min_{s\in\mathcal{S}} P(\mathcal{X}_H|s)} \leq \mathrm{e}^{\varepsilon}. \tag{34}$$

证明. 充分条件：考虑一个 X-不变的随机化，其中 $r(y|x) = \mathcal{R}(y), \quad \forall x \in \mathcal{X}_H$ 和 $y \in \mathcal{Y}_H$。如果式 (34) 成立，那么对于所有 $s, s' \in \mathcal{S}$，我们有

$$\begin{aligned}
\frac{P(\mathcal{X}_H|s)}{P(\mathcal{X}_H|s')} \leq \frac{\max_{s\in\mathcal{S}} P(\mathcal{X}_H|s)}{\min_{s\in\mathcal{S}} P(\mathcal{X}_H|s)} \leq \mathrm{e}^{\varepsilon} \Rightarrow \\
P(\mathcal{X}_H|s) \leq P(\mathcal{X}_H|s')\mathrm{e}^{\varepsilon} \Rightarrow \\
\mathcal{R}(y)P(\mathcal{X}_H|s) \leq \mathcal{R}(y)P(\mathcal{X}_H|s')\mathrm{e}^{\varepsilon} \Rightarrow \\
\sum_{x\in\mathcal{X}_H} r(y|x)P_{X|S}(x|s) \leq \sum_{x\in\mathcal{X}_H} r(y|x)P_{X|S}(x|s')\mathrm{e}^{\varepsilon} \Rightarrow \\
P_{Y|S}(y|s) \leq P_{Y|S}(y|s')\mathrm{e}^{\varepsilon}.
\end{aligned}$$

对于必要条件，注意，对所有 s、$s' \in \mathcal{S}$ 和 $y \in \mathcal{Y}_H$，我们有

$$P_{Y|S}(y|s) \leq \mathrm{e}^{\varepsilon} P_{Y|S}(y|s') \Rightarrow \sum_{x\in\mathcal{X}_H} r(y|x)P_{X|S}(x|s) \leq \mathrm{e}^{\varepsilon} \sum_{x\in\mathcal{X}_H} r(y|x)P_{X|S}(x|s'),$$

然后，对等式两边的所有 $y \in \mathcal{Y}_H$ 求和，可得

$$\begin{aligned}
&\sum_{x\in\mathcal{X}_H} P_{X|S}(x|s) \underbrace{\sum_{y\in\mathcal{Y}_H} r(y|x)}_{=1} \leq \mathrm{e}^{\varepsilon} \sum_{x\in\mathcal{X}_H} P_{X|S}(x|s') \underbrace{\sum_{y\in\mathcal{Y}_H} r(y|x)}_{=1} \\
&\Rightarrow P(\mathcal{X}_H|s) \leq P(\mathcal{X}_H|s')\mathrm{e}^{\varepsilon} \Rightarrow \frac{P(\mathcal{X}_H|s)}{P(\mathcal{X}_H|s')} \leq \mathrm{e}^{\varepsilon}. \qquad (35)
\end{aligned}$$

由于式（35）对所有 s、$s' \in \mathcal{S}$ 均成立，我们有

$$\max_{s,s'\in\mathcal{S}} \frac{P(\mathcal{X}_H|s)}{P(\mathcal{X}_H|s')} = \frac{\max_{s\in\mathcal{S}} P(\mathcal{X}_H|s)}{\min_{s\in\mathcal{S}} P(\mathcal{X}_H|s)} \leq \mathrm{e}^{\varepsilon}.$$

□

APPENDIX C

1）对于 ℓ_1-提升，我们有

$$\Lambda_{\ell_1}(y) = \sum_{s\in\mathcal{S}} P_S(s)|l(s,y) - 1| \leq \sum_{s\in\mathcal{S}} P_S(s)|\Lambda(y) - 1| = \Lambda(y) - 1 \leq \mathrm{e}^{\varepsilon_u} - 1.$$

2）对于 χ^2-提升，我们有

$$\Lambda_{\chi^2}(y) = \sum_{s\in\mathcal{S}} P_S(s)\big(l(s,y) - 1\big)^2 \leq \sum_{s\in\mathcal{S}} P_S(s)\left(\Lambda(y) - 1\right)^2 = \left(\Lambda(y) - 1\right)^2 \leq \left(\mathrm{e}^{\varepsilon_u} - 1\right)^2.$$

3）对于 α-提升，我们有

$$\Lambda_{\alpha}^{S}(y) = \left(\sum_{s\in\mathcal{S}} P_S(s)l(s,y)^{\alpha}\right)^{1/\alpha} \leq \left(\sum_{s\in\mathcal{S}} P_S(s)\Lambda(y)^{\alpha}\right)^{1/\alpha} = \Lambda(y) \leq \mathrm{e}^{\varepsilon_u}.$$

附录D

如果 $s_y = \underset{s\in\mathcal{S}}{\operatorname{argmax}}\ l(s,y)$，那么我们有 $\Lambda(y) = l(s_y, y)$。回想一下，$\bar{y} = \underset{y\in\mathcal{Y}}{\operatorname{argmax}}[\Lambda(y)]$。

1) 当 $\max_{y\in\mathcal{Y}} \Lambda_{\ell_1}(y) \leq \varepsilon$ 时，对于所有 $y \in \mathcal{Y}$，我们有

$$\Lambda_{\ell_1}(y) = \sum_{s\in\mathcal{S}} P_S(s)|l(s,y) - 1| \leq \varepsilon \Rightarrow P_S(s_y)|l(s_y,y) - 1| = P_S(s_y)(\Lambda(y) - 1) \leq \varepsilon,$$

由此得到

$$\max_{y\in\mathcal{Y}} \Lambda(y) \leq \frac{\varepsilon}{P_S(s_{\bar{y}})} + 1.$$

2）当对于所有 $y \in \mathcal{Y}$，$\max_{y\in\mathcal{Y}} \Lambda_{\chi^2}(y) \leq \varepsilon$ 时，我们有

$$\Lambda_{\chi^2}(y) = \sum_{s\in\mathcal{S}} P_S(s)\left(l(s,y) - 1\right)^2 \leq \varepsilon \Rightarrow P_S(s_y)\left(l(s_y,y) - 1\right)^2 = P_S(s_y)(\Lambda(y) - 1)^2 \leq \varepsilon,$$

由此可得

$$\max_{y\in\mathcal{Y}}\Lambda(y)\le\sqrt{\frac{\varepsilon}{P_S(s_{\bar{y}})}}+1.$$

3) 当 $\max_{y\in\mathcal{Y}}\Lambda_\alpha^S(y)\le\varepsilon$ 时，对于所有 $y\in\mathcal{Y}$，我们有

$$\Lambda_\alpha^S(y)=\left(\sum_{s\in\mathcal{S}}P_S(s)l(s,y)^\alpha\right)^{1/\alpha}\le\varepsilon\Rightarrow P_S(s_y)l(s_y,y)^\alpha=P_S(s_y)\Lambda(y)^\alpha\le\varepsilon^\alpha,$$

由此可得

$$\max_{y\in\mathcal{Y}}\Lambda(y)\le\frac{\varepsilon}{P_S(s_{\bar{y}})^{\frac{1}{\alpha}}}.$$

附录 E

由于满足 $(\varepsilon_l,\varepsilon_u)$-ALIP，对于所有 $y\in\mathcal{Y}$，我们有 $\mathrm{e}^{-\varepsilon_u}\le\frac{1}{l_s^{-1}(\cdot,y)}\le\mathrm{e}^{\varepsilon_l}$ 且 $\max_s\left(l_s^{-1}(\cdot,y)\right)=\Psi^{-1}(y)$。1) 对于 ℓ_1-提升逆，我们有

$$\Psi_{\ell_1}(y)=\sum_{s\in\mathcal{S}}P_S(s)\left|\frac{1}{l(s,y)}-1\right|\le\sum_{s\in\mathcal{S}}P_S(s)\left|\frac{1}{\Psi(y)}-1\right|=\frac{1}{\Psi(y)}-1\le\mathrm{e}^{\varepsilon_l}-1.$$

2) 对于 χ^2-提升逆，我们有

$$\Psi_{\chi^2}(y)=\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{l(s,y)}-1\right)^2\le\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{\Psi(y)}-1\right)^2=\left(\frac{1}{\Psi(y)}-1\right)^2\le\left(\mathrm{e}^{\varepsilon_l}-1\right)^2.$$

3) 对于 α-提升逆，我们有

$$\Psi_\alpha^S(y)=\left(\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{l(s,y)}\right)^\alpha\right)^{\frac{1}{\alpha}}\le\left(\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{\Psi(y)}\right)^\alpha\right)^{\frac{1}{\alpha}}=\frac{1}{\Psi(y)}\le\mathrm{e}^{\varepsilon_l}.$$

附录 F

若 $s_y=\operatorname{argmin}_s l(s,y)$，则有 $\Psi(y)=l(s_y,y)$。回忆一下，$\underline{y}=\operatorname{argmin}_y[\Psi(y)]$.

1) 当 $\max_{y\in\mathcal{Y}}\Psi_{\ell_1}(y)\le\varepsilon$ 时，对于所有 $y\in\mathcal{Y}$，有

$$\Psi_{\ell_1}(y)=\sum_{s\in\mathcal{S}}P_S(s)\left|\frac{1}{l(s,y)}-1\right|\le\varepsilon\Rightarrow P_S(s_y)\left|\frac{1}{l(s_y,y)}-1\right|=P_S(s_y)\left(\frac{1}{\Psi(y)}-1\right)\le\varepsilon,$$

由此可得

$$\min_{y\in\mathcal{Y}}\Psi(y)\ge\frac{P_S(s_{\underline{y}})}{\varepsilon+P_S(s_{\underline{y}})}.$$

2) 当 $\max_{y\in\mathcal{Y}}\Psi_{\chi^2}(y)\le\varepsilon$ 时，对于所有 $y\in\mathcal{Y}$，有

$$\Psi_{\chi^2}(y)=\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{l(s,y)}-1\right)^2\le\varepsilon\Rightarrow P_S(s_y)\left(\frac{1}{l(s_y,y)}-1\right)^2=P_S(s_y)\left(\frac{1}{\Psi(y)}-1\right)^2\le\varepsilon,$$

由此可得

$$\min_{y\in\mathcal{Y}}\Psi(y)\ge\frac{\sqrt{P_S(s_{\underline{y}})}}{\sqrt{\varepsilon}+\sqrt{P_S(s_{\underline{y}})}}.$$

3）当对于所有 $y\in\mathcal{Y}$ 均有 $\max_{y\in\mathcal{Y}}\Psi_\alpha^S(y)\le\varepsilon$ 时，我们有

$$\Psi_\alpha^S(y)=\left(\sum_{s\in\mathcal{S}}P_S(s)\left(\frac{1}{l(s,y)}\right)^\alpha\right)^{1/\alpha}\le\varepsilon\Rightarrow P_S(s_y)\left(\frac{1}{l(s_y,y)}\right)^\alpha=P_S(s_y)\left(\frac{1}{\Psi(y)}\right)^\alpha\le\varepsilon^\alpha,$$

从而导致

$$\min_{y\in\mathcal{Y}}\Psi(y)\ge\varepsilon^{-1}P_S(s_{\underline{y}})^{\frac{1}{\alpha}}.$$

参考文献

[1] C. Dwork、F. McSherry、K. Nissim 和 A. Smith，“私有数据分析中将噪声校准至敏感度”，载于《密码学理论》，S. Halevi 和 T. Rabin 编。柏林，海德堡：Springer Berlin Heidelberg，2006年，第265–284页。[2] C. Dwork，“差分隐私”，载于第33届自动机、语言与编程国际研讨会，第II部分（ICALP 2006），计算机科学讲义丛书，第4052卷。Springer Verlag，2006年7月，第1–12页。[3] ——，“差分隐私”，《密码学与安全百科全书》，第338–340页，2011年。[4] S. P. Kasiviswanathan、H. K. Lee、K. Nissim、S. Raskhodnikova 和 A. Smith，“我们能以隐私保护方式学到什么？”，《SIAM计算杂志》，第40卷，第3期，第793–826页，2011年。[5] J. C. Duchi、M. I. Jordan 和 M. J. Wainwright，“局部隐私与统计极小极大速率”，载于第54届IEEE计算机科学基础年度研讨会论文集，2013年，第429–438页。[6] P. Kairouz、S. Oh 和 P. Viswanath，“局部差分隐私的极值机制”，载于《神经信息处理系统进展》，第4卷，2014年1月，第2879–2887页。[7] A. D. Sarwate 和 L. Sankar，“局部差分隐私的率失真视角”，载于Allerton通信、控制与计算年会论文集，2014年，第903–908页。[8] K. Kalantari、L. Sankar 和 A. D. Sarwate，“差分隐私和汉明失真下稳健的隐私-效用权衡”，《IEEE信息取证与安全汇刊》，第13卷，第11期，第2816–2830页，2018年。[9] L. Sankar、S. R. Rajagopalan 和 H. V. Poor，“数据库中的效用-隐私权衡：一种信息论方法”，《IEEE信息取证与安全汇刊》，第8卷，第6期，第838–852页，2013年。[10] B. Jiang、M. Li 和 R. Tandon，“具有局部化信息隐私的上下文感知数据聚合”，载于2018年IEEE通信与网络安全会议（CNS），2018年，第1–9页。[11] A. Makhdoumi、S. Salamatian、N. Fawaz 和 M. Médard，“从信息瓶颈到隐私漏斗”，载于2014年IEEE信息论研讨会（ITW 2014），2014年11月，第501–505页。[12] S. Salamatian、F. du Pin Calmon、N. Fawaz、A. Makhdoumi 和 M. Médard，《隐私-效用权衡与隐私漏斗》，2020年，见 http://www.mit.edu/~salmansa/files/privacy_TIFS.pdf。[13] I. Issa、S. Kamath 和 A. B. Wagner，“信息泄露的操作性度量”，载于2016年信息科学与系统年度会议，普林斯顿，新泽西州，2016年，第234–239页。[14] I. Issa、S. Kamath 和 A. B. Wagner，“香农密码系统的最大泄露最小化”，载于2016年IEEE信息论国际研讨会（ISIT），2016年，第520–524页。[15] I. Issa、A. B. Wagner 和 S. Kamath，“信息泄露的操作性方法”，《IEEE信息论汇刊》，第66卷，第3期，第1625–1657页，2020年3月。[16] J. Liao、O. Kosut、L. Sankar 和 F. P. Calmon，“一种用于信息泄露的可调节度量”，载于IEEE信息论国际研讨会（ISIT）。IEEE，2018年，第701–705页。[17] F. du Pin Calmon 和 N. Fawaz，“抵御统计推断的隐私”，载于第50届Allerton通信、控制与计算年会（Allerton）。IEEE，2012年，第1401–1408页。[18] B. Jiang、M. Li 和 R. Tandon，“具有有界先验的局部信息隐私”，载于2019年IEEE国际通信会议（ICC），2019年，第1–7页。[19] M. Seif、R. Tandon 和 M. Li，“用于局部信息隐私的上下文感知拉普拉斯机制”，载于2019年IEEE信息论研讨会（ITW），2019年，第1–5页。[20] B. Jiang、M. Li 和 R. Tandon，“局部信息隐私及其在隐私保护数据聚合中的应用”，《IEEE可信与安全计算汇刊》，第1–1页，2020年。[21] B. Jiang、M. Seif、R. Tandon 和 M. Li，“上下文感知局部信息隐私”，《IEEE信息取证与安全汇刊》，第16卷，第3694–3708页，2021年。[22] N. Ding、Y. Liu 和 F. Farokhi，“局部差分隐私和对数提升的线性约简方法”，载于2021年IEEE信息论国际研讨会（ISIT），2021年，第551–556页。[23] H. Hsu、S. Asoodeh 和 F. d. P. Calmon，“信息论隐私监视器”，载于IEEE信息论国际研讨会论文集，巴黎，法国，2019年，第552–556页。[24] P. Sadeghi、N. Ding 和 T. Rakotoarivelo，“论信息论隐私监视器的性质与优化”，载于IEEE信息论研讨会论文集，2020年。[25] M. A. Zarrabian、N. Ding、P. Sadeghi 和 T. Rakotoarivelo，“提升监视器隐私机制中的效用”，载于ICASSP 2022—2022年IEEE声学、语音与信号处理国际会议（ICASSP）。IEEE，2022年，第2979–2983页。[26] B. Razeghi、F. Calmon、D. Gunduz 和 S. Voloshynovskiy，“论完美混淆：局部信息几何分析”，arXiv预印本 arXiv:2009.04157，2020年。[27] M. Lopuhaä-Zwakenberg、H. Tong 和 B. Škori´c，“具有差分隐私保证的隐私漏斗数据净化协议”，《安全进展国际期刊》，第13卷，第3、4期，第162–174页，2021年2月。[28] A. Zamani、T. J. Oechtering 和 M. Skoglund，“具有非零泄漏和不可逆泄露矩阵的数据披露”，《IEEE信息取证与安全汇刊》，第17卷，第165–179页，2022年。[29] ——，“强 χ^2 16， 2312 2325, -私 2021 有数据披露的设计框架”，《IEEE信息取证与安全汇刊》，第 pp. – 页。[30] N. Ding、M. A. Zarrabian 和 P. Sadeghi，“α-信息论隐私监视器与最优隐私化方案”，载于IEEE信息论国际研讨会论文集，2021年，第2584–2589页。[31] B. Rassouli 和 D. Gunduz，“以全变差距离作为隐私度量的最优效用-隐私权衡”，《IEEE信息取证与安全汇刊》，2019年。[32] S. Asoodeh、M. Diaz、F. Alajaji 和 T. Linder，“隐私约束下的估计效率”，《IEEE信息论汇刊》，第65卷，第3期，第1512–1534页，2018年。[33] B. Rassouli、F. E. Rosas 和 D. Gunduz，“完美样本隐私下的数据披露”，arXiv预印本 arXiv:1904.01711，2019年。[34] Y. Liu、P. Sadeghi、F. Arbabjolfaei 和 Y. H. Kim，“分布式索引编码的容量定理”，《IEEE信息论汇刊》，第66卷，第8期，第4653–4680页，2020年。[35] H. Wang、L. Vo、F. P. Calmon、M. Médard、K. R. Duffy 和 M. Varia，“具有估计保证的隐私”，《IEEE信息论汇刊》，第65卷，第12期，第8025–8042页，2019年。