arXiv:2303.02916v1 [cs.IR] 6 Mar 2023

保护隐私的公平项目排序

Jia Ao Sun[1,2], Sikha Pentyala[1,3],Martine De Cock[3,4],和 Golnoosh Farnadi[1,2,5]

[1] Mila -魁北克人工智能研究所，蒙特利尔QC 加拿大[2] 蒙特利尔大学，蒙特利尔QC 加拿大[3] 华盛顿大学，塔科马 WA 美国[4] 根特大学，根特 比利时[5] 蒙特利尔高等商学院，蒙特利尔QC 加拿大
{sunjiaao,farnadig}@mila.quebec
{sikha,mdecock}@uw.edu

摘要。 世界各地的用户每天都以排名的形式访问海量的精选数据。这种便利的数据获取方式所产生的社会影响已经得到研究，相关工作也提出并推动了排名公平性的各种理念。当前的公平项目排序计算方法依赖于将用户数据披露给集中式服务器，这给用户带来了隐私问题。本研究首次在排名中同时推进生产者（项目）公平性与消费者（用户）隐私方面的研究，探索引入隐私保护技术，具体包括差分隐私和安全多方计算。我们的工作将摊销注意力排名机制的公平性扩展为隐私保护机制，并评估其对隐私、公平性和排名质量的影响。使用真实世界数据集进行的实验结果表明，与明文状态下的排序机制相比，我们能够有效保护用户隐私并缓解项目的不公平性，同时无需在排名质量方面作出额外牺牲。

关键词： 排序 · 隐私 · 公平性。

1 引言

信息系统，例如用于搜索检索和推荐的信息系统，已成为我们日常生活中无处不在的一部分。这些系统会向用户提供经过筛选的信息，例如社交媒体上发布的内容或网页；也会按照与用户最相关的方式组织信息，帮助用户决定买什么、看什么或聘用谁。这些结果通常以排序列表的形式呈现。为了最大限度地提升系统对每位用户的效用，排序列表会按照与用户的相关性（依据某种分数或评级）从高到低排列。因此，用户往往会把大部分注意力放在排序列表中排名最高的项目上，从而产生位置偏差[13,12]。对于单个排序列表（为单个用户或单个查询生成），每个项目获得的注意力会比其相关性下降得更快，即排名较低的项目处于不利地位，获得的注意力与其相关性相比

少得不成比例。当以这种方式连续生成一系列排序列表时，排名较高的项目相较于其相关性会获得越来越多、且不成比例的注意力。这会对主要利益相关方——信息系统中的项目提供者，又称生产者——造成经济和社会影响，导致经济差距、对代表性不足的生产者的偏差，以及不健康的市场 [14,17]。

文献中已有研究提出了缓解排名不公平性的方法 [30,18,25,31,19]。在我们的工作中，我们重点关注通过重新排序排序列表来公平分配曝光度的后处理技术 [24,3]。这些方法假设用户的排名或偏好可供某个中央实体使用，后者随后可以应用后处理技术，实现项目之间的公平性。集中存储用户数据可能导致隐私泄露，甚至引发蓄意侵犯隐私的行为，例如公司破产时定期出售数据 [4]。人们日益认识到需要加强用户隐私保护，同时也必须遵守《通用数据保护条例》等法规 [6]，这推动了隐私增强技术（PETs）在推荐系统中的广泛应用 [11,29,1,6,28]。据我们所知，目前尚无研究探讨如何在排名系统中实现生产者（亦即 项目）的公平性，同时保护消费者（亦即用户）的隐私。本文将探讨这一在文献中研究不足的领域。

我们研究这样一个问题：每位用户（客户端） u_l 都拥有一个 ρ_l 项目d_1^l，d_2^l、.....、d_i^l、.....、d_n^l 列表，该列表以保护隐私的方式生成，并根据相关性进行排序。在偏差缓解的后处理阶段，我们希望调整每位用户的排名 ρ_l ，以优化摊销注意力公平性 [3] ，而无需任何用户向集中式实体披露 ρ_l 。借助安全多方计算（安全多方计算），可以实现这一目标，即让每个客户端加密其数据并将其发送给一组多方计算服务器，由多方计算服务器在加密数据上执行重排序所需的全部计算，然后将结果返回给客户端进行解密。尽管这种方法能够保留端到端隐私，并生成与 Biega 等人的偏差缓解方法 [3] 在明文中（即不进行任何加密）产生的相同排名，但其计算和通信开销对于实际应用而言将大得难以接受。因此，我们提出了一种更具可扩展性的方法，将安全多方计算用于保护输入隐私，并结合差分隐私（差分隐私）来保护输出隐私。在我们的方案中，多方计算服务器存储中间结果，然后使用差分隐私噪声对其进行扰动，客户端随后利用这些结果执行本地计算。我们通过在三个真实世界数据集上进行实验，展示了所提方案的适用性。实验结果表明，在确保用户隐私的同时，可以改善项目的公平性，而无需进一步牺牲排名质量。

[6] 欧盟《通用数据保护条例》 https://gdpr-info.eu/

2 预备知识

2.1 排序公平性

为最大化效用，排序算法会生成项目列表，并按照其对查询或用户的预测相关性水平进行排序。相关性最高的项目位于列表顶部，并获得最多的曝光度。排名公平性关注如何在已排名项目之间分配曝光度，以减轻位置偏差所造成的影响。在这一背景下，人们提出了许多公平性概念 [30,31,5,22,24]。本文考察一种基于项目所获得注意力的公平性概念；正如 Biega 等人 [3]所提出的，这种注意力取决于项目的曝光度。

摊销注意力公平性（EOAA）Biega 等人提出了摊销注意力公平性这一公平性概念，以实现一组项目 $\mathcal{D} = \{d_1, d_2, \ldots, d_i, \ldots, d_n\}$ 在面向用户 u_1、u_2、.....、u_l、u_L的一系列基于相关性的排序 ρ_1、ρ_2、.....、ρ_l、.....、ρ_L 中的摊销个体公平性 [3]。项目 d_i 在排序 ρ_l 中的位置会影响其获得的注意力。若在一系列排序中进行摊销后，每个项目 d_i 获得的累积注意力 A_i 与其累积相关性 R_i成正比，则实现了 EOAA。Biega 等人通过计算 A_i 与 R_i 之间绝对差值的总和，为 $i = 1 \ldots n$ 定义了这一公平性概念的度量，如公式 1 所示：

$$unfairness(\rho_1, ..., \rho_L) = \sum_{i=1}^{n} |A_i - R_i| = \sum_{i=1}^{n} \left| \sum_{l=1}^{L} a_i^l - \sum_{l=1}^{L} r_i^l \right|. \tag{1}$$

对于每个项目 d_i，r_i^l 是其面向用户 u_l的相关性分数，而 a_i^l 是它在排序 ρ_l中获得的注意力。Biega 等人提出，通过依次对每个基于相关性的排序进行重排序，生成 ρ_1^*，ρ_2^*、.....、ρ_l^*、.....、ρ_L^*，从而提升一系列基于相关性的排序 ρ_1，ρ_2、.....、ρ_l、.....、ρ_L 的 EOAA。为重排序 ρ_l，并考虑先前计算出的重排序结果 ρ_1^*，ρ_2^*、.....、ρ_{l-1}^*，需要求解以下后处理线性规划（整数线性规划）：

$$\text{Minimize} \sum_{i=1}^{n} \sum_{j=1}^{n} \left| A_i^{l-1} + \hat{w}_j - (R_i^{l-1} + \hat{r}_i^l) \right| \cdot X_{i,j} \tag{2}$$

$$\text{Subject to} \sum_{j=1}^{k} \sum_{i=1}^{n} \frac{2^{\hat{r}_i^l} - 1}{\log_2(j+1)} X_{i,j} \geq \theta \cdot DCG(\rho_l)@k \tag{3}$$

$$X_{i,j} \in \{0, 1\}, \forall_{i,j} \text{ and } \sum_i X_{i,j} = 1, \forall_j \text{ and } \sum_j X_{i,j} = 1, \forall_i. \tag{4}$$

该整数线性规划求解 n^2 决策变量$X_{i,\ j}$ 这些变量表示排名 ρ_l中项目的重排序 ρ_l^*。A_i^{l-1} 和 R_i^{l-1} 分别表示项目 d_i在重新排名 ρ_1^*，ρ_2^*，.....，ρ_{l-1}^*中的累积注意力和相关性。$\hat{}w_j$ 是归一化后的

将项目放置在位置 j时的注意力权重，基于 [3]中假设的几何注意力模型 $w_j = 0.5(0.5)^{j-1}$，计算为 $\hat{w}_j = w_j / \sum_{t=1}^{n} w_t$。$\hat{r}_i^l$ 是 r_i^l的归一化相关性分数，计算为 $\hat{r}_i^l = \frac{r_i^l - r_{\min}}{r_{\max} - r_{\min}} \Big/ \sum_{t=1}^{n} \frac{r_t^l - r_{\min}}{r_{\max} - r_{\min}}$。$r_{\max}$ 和 $r_{\min}$ 分别是用户对某个项目可能给出的最高和最低相关性分数。系数 $\left| A_i^{l-1} + w_j - (R_i^{l-1} + r_i^l) \right|$ 表示在当前重排序中将项目 d_i 放置在位置 j 时的不公平性度量。公式 3 中的约束根据折扣累计增益（DCG）限制重排序中前 k 个项目的质量，使其不低于原始基于相关性的排序中前 k 个项目的 DCG 的 $0 \leq \theta \leq 1$ 倍。公式 4 中的约束规定，n^2 决策变量 $X_{i,j}$ 为二元变量，并且对于所有 i，每个 j 恰有一个 1；对于所有 j，每个 i 也恰有一个 1。$X_{i,j} = 1$ 表示项目 d_i 被放置在位置 j，而 $X_{i,j} = 0$ 则表示否则。

重排序的质量 ρ_l^* 以其偏离原始基于相关性的排序 ρ_l的程度来衡量。在公式 5 中，该程度量化为归一化折扣累计增益(ρ_l, ρ_l^*)，其中 $DCG(\rho_l^*)$通过 $DCG(\rho_l)$进行归一化。

$$NDCG(\rho_l, \rho_l^*) = \frac{DCG(\rho_l^*)}{DCG(\rho_l)} \tag{5}$$

归一化折扣累计增益的最大值为 1，在 $\rho_l = \rho_l^*$时取得；如果相关性分数相同的项目彼此之间进行随机打乱，也会取得该最大值。

2.2 隐私增强技术（隐私增强技术）

差分隐私（差分隐私）差分隐私为数据集上的计算结果提供形式化保证：D 单个用户的参与对结果的影响可以忽略不计，从而通过合理推诿实现隐私保护 [9]。形式化地说，随机算法 $\mathcal{F}$ 在满足以下条件时提供 ϵ-差分隐私：对于所有相邻数据集对 D和 D'（即相差一个实体的数据集），以及 $\mathcal{F}$取值范围的所有子集 S，

$$\mathrm{P}(\mathcal{F}(D) \in S) \leq e^{\epsilon} \cdot \mathrm{P}(\mathcal{F}(D') \in S), \tag{6}$$

其中，ϵ 是隐私预算或隐私损失。ϵ的值越小，隐私保证越强。ϵ-DP 算法 $\mathcal{F}$ 通常通过向算法 $\mathcal{F}^*$ 添加与敏感度 成比例的噪声来构造，其中敏感度衡量底层数据集发生变化时对 $\mathcal{F}^*$输出的最大影响。在我们的论文中，$\mathcal{F}^*$ 会聚合多个用户对项目的相关性分数和注意力权重。传统的差分隐私范式——全局差分隐私——假设存在一位中央管理者，负责收集用户数据，并在披露计算所得的聚合值时，向输入、输出或两者注入可控噪声。尽管这种模型提供了输出隐私，但它要求用户向中央实体披露其隐私数据。为了避免披露用户敏感信息的需要，本文通过一组运行安全多方计算协议的不可信服务器（见下文）来模拟全局差分隐私范式中的中央管理者。

安全多方计算（MPC）MPC [7] 是一个统称，涵盖了能够对加密数据进行计算的密码学方法。我们采用多方计算即服务范式：每个数据持有者将其输入数据中的每个值 x 加密，方法是将其转换为所谓的秘密份额，随后将这些份额分发给一组多方计算服务器。虽然合并所有份额即可轻易重构原始值 x，但任何单个多方计算服务器都无法获知 x的值。接下来，多方计算服务器共同执行协议，对秘密共享值进行计算，从而得到所需输出值的秘密共享（在我们的论文中，该输出是经噪声扰动以提供差分隐私的聚合不公平性度量）。多方计算关注的是协议执行过程中遭到对手攻击的情形；对手可能破坏一个或多个参与方，以获取隐私信息或导致计算结果不正确。本文使用的安全多方计算协议旨在防止此类攻击得逞，并已通过数学证明，能够保证输入隐私和正确性。

威胁模型 对手可以破坏任意数量的参与方。在不诚实多数 设置中，半数或更多参与方可能遭到破坏；而在诚实多数 设置中，超过半数的参与方是诚实的（未遭到破坏）。此外，对手可以是半诚实 对手，也可以是恶意 对手。被半诚实或“被动”对手破坏的参与方会正确遵循协议指令，但会试图获取额外信息；而被恶意或“主动”对手破坏的参与方则可能偏离协议指令。本文使用的协议具有足够的通用性，既可用于不诚实多数设置，也可用于诚实多数设置，并支持被动或主动对手。具体而言，只需更改底层的多方计算方案，使其符合所需的安全设置即可实现这一点。

多方计算通常在模 q 的整数上进行，即也就是说，在环 $\mathbb{Z}_q$ 中进行。例如，在一个广为人知的、具有被动对手的不诚实多数两方计算（2PC）设置中，数据持有者将其输入数据转换为 $x = x_0 + x_1$ 模 q，并将 x_0 发送给多方计算服务器 S_0，将 x_1 发送给 S_1。在全文中，我们使用 $[\![x]\!] = (x_0, x_1)$ 作为对 x 进行秘密共享的简写。如果服务器从另一数据持有者处接收到某个值 y 的秘密份额 y_0 和 y_1，那么服务器可以将 $x+y$ 的秘密共享计算为 $[\![x+y]\!] = (x_0+y_0, x_1+y_1)$，而无需获知 x、y 或它们的和。除加法外，我们还使用一种 MPC 协议 π_{LAP}，使多方计算服务器能够对从拉普拉斯分布中抽取的噪声进行秘密共享采样。π_{LAP} 要复杂得多，除了对服务器自身本地份额进行操作外，还涉及多方计算服务器之间的通信。详情请参见 [20]。

3 相关工作

3.1 排名公平性

排名公平性领域的大多数研究都聚焦于如何公平地向排序列表中的元素分配曝光度。排序列表中的元素可以是人或项目（例如，内容、产品、地点）。许多相关研究

都围绕群体公平性展开，即理想情况下，应在依据受保护属性（如性别或种族）划分的不同群体之间平等分配曝光度。例如，Yang 和 Stoyanovich [30]提出将传统的统计均等公平性概念扩展到排序系统：在排序中，一个人是否属于受保护群体，不应影响其排名位置。Zehlike 和 Castillo [31] 提出了一种公平的前-k排序算法，遵循平权行动的公平理念，确保每个前-k排序（前 10 名、前 20 名等）中至少包含一定数量的受保护群体成员。Celis 等人 [5] 提出了一种解决约束排序最大化问题的算法：限制排序中每个受保护群体的敏感项目数量，避免任何一个群体占据主导地位。Sapiezynski 等人 [22]也采用了统计均等，但使用几何分布来模拟用户注意力，作为曝光度的替代指标。Singh 和 Joachims [24] 引入了排名中的曝光公平性，并提出使用线性规划，在满足群体公平性约束的前提下，优化排序的最大效用。然而，针对排名中单项公平性的研究仍然有限。其中一项研究是 Biega 等人 [3] 提出的注意力公平性，旨在通过按项目相关性比例分配注意力，在一系列排序中实现摊销公平性。我们的工作扩展了 Biega 等人 [3] 提出的重排序方法，在排序机制的各个阶段实施隐私保护措施。

3.2 隐私保护排序系统

此前关于隐私保护学习排序（LTR）系统的研究采用了多种隐私增强技术。Dehghani 等人 [8] 采用了模仿学习，仅共享基于敏感数据训练的模型，而不共享数据本身。此外，作为差分隐私保证的一部分，聚合过程中会加入拉普拉斯噪声。Yang 等人 [29] 采用了信息论隐私方法，即根据数据失真预算对数据进行混淆。Kharitonov [16]采用了结合进化策略优化的联邦学习方案，随后又加入了本地差分隐私。Wang 等人 [27]将 Kharitonov 的工作扩展到更大的数据集，并发现与其他非隐私保护的在线学习排序系统相比，其效用显著降低。随后，Wang 等人 [26] 采用了联邦学习方案和本地差分隐私，与 Kharitonov [16], 的方法类似，但改用成对可微梯度下降（PDGD）优化方法。Ge 等人 [11] 在其 PrivItem2Vec 模型中采用了 Paillier 同态加密算法。在此前的隐私保护排序系统研究中，尚无工作将安全多方计算与差分隐私结合使用。

3.3 公平且隐私保护的排序系统

显然，排名公平性以及排序系统中的隐私保护方法都已得到充分研究；然而，关于排序系统中公平性与隐私交叉领域的研究却十分匮乏。Resheff 等人 [21] 在其推荐系统中采用隐私对抗训练，以获得能够混淆用户敏感属性的用户

表示。这种方法着重提升群体公平性，并通过防止隐式私人信息攻击来保护部分用户隐私。Sato [23] 提出了一种独立于集中式推荐系统的本地排序系统框架，用户可以通过为自己的偏好设定公平性约束，自行对收到的排名进行后处理。其隐私保护方法是由每位用户开发自己的推荐系统。然而，这种方法的计算成本极高，而且许多用户的设备没有足够的处理能力来维持这些系统。这两项工作都针对用户的受保护属性来解决隐私和公平性问题，但据我们所知，迄今尚无研究关注项目获得的注意力与其相关性之间的关系所涉及的隐私和公平性问题。

4 方法

4.1 问题描述

我们考虑一种回归式推荐模型 $\mathcal{M}$，该模型以保护隐私的方式（例如 [28,16]）进行训练，即，模型不会泄露任何训练数据的信息。 $\mathcal{M}$ 该模型部署在每个用户 u_l 处，用于预测其在全局项目集 $\mathcal{D}$ 上的相关性分数 $\mathbf{r}^l = (r_1^l、 r_2^l、 \ldots\ldots、 r_i^l、 \ldots\ldots、 r_n^l)$，其中$r_i^l = \mathcal{M}(u_l、 d_i)$。在此过程中，用户的原始数据——例如其偏好、人口统计信息、嵌入等——不会向任何人披露。用户 u_l 的基于相关性的排序 ρ_l 是按照相关性分数降序排列的项目列表。

第 2.1 节所述的后处理技术假设中央服务器 S能够访问所有用户的基于相关性的排名 $\rho_1、 \rho_2、 \ldots\ldots、 \rho_l、 \ldots\ldots、 \rho_L$，并将其重排序为 $\rho_1^*、 \rho_2^*、 \ldots\ldots、 \rho_l^*、 \ldots\ldots、 \rho_L^*$，以实现摊销注意力公平性，同时不使排序效用损失超过设定阈值。我们将这种设置称为集中式设置，它会导致用户敏感信息泄露给中央服务器 S，包括：

(P_1) 用户对所有项目的偏好，以相关性分数的形式表示；(P_2) 用户最可能感兴趣的前-k 个项目；以及(P_3) 用户最可能感兴趣的前-k 个项目的排序。

下面我们将介绍如何调整上述后处理方法，以解决隐私问题（(P_1)–(P_3)），从而实现项目的个体公平性并保护用户的隐私。

4.2 所提方法

我们方法的核心观察是，除公式 2 中的 A_i^{l-1} 和 R_i^{l-1} 的值外，每个用户 u_l 都拥有解决 ILP 所需的全部信息，可以将其原始排名 ρ_l 重排序ρ_l^*为 A_i^{l-1} 和 R_i^{l-1} 分别是项目 d_i在重新排名中的累积注意力和相关性

[7] 图片改编自 https://sepior.com/mpc-blog

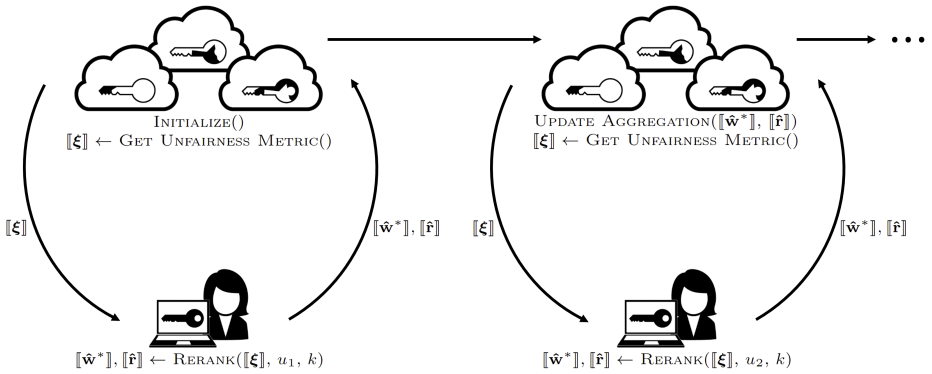


图 1：隐私保护公平项目排序算法流程图[7]

ρ_1^*，ρ_2^*、.....、ρ_{l-1}^*，即，A_i^{l-1}和 R_i^{l-1}的值取决于用户 u_1、.....、u_{l-1}的敏感信息；我们既不希望将这些信息披露给用户 u_l，也不希望披露给中央服务器（集中式设置即是如此）。因此，在我们的解决方案中，我们维护 A_i^{l-1} 和 R_i^{l-1} 的加密版本，其初始值均为 0（参见算法 1 中的初始化过程），并在每个用户完成 ILP计算后，以保护隐私的方式进行更新。更准确地说，在任何时刻，都没有任何单个实体知道 A_i^{l-1} 和 R_i^{l-1} 的当前值。相反，这些值会被拆分为秘密份额，并分发到多方计算服务器；这些服务器可以联合执行操作来更新份额，同时始终无法获知输入的真实值或计算结果。图1展示了我们解决方案的高层流程，算法1给出了伪代码，下面将对此进行更详细的解释。我们使用$\mathbf{A}^{l-1}$ 和$\mathbf{R}^{l-1}$ 分别表示向量$[A_1^{l-1},\ldots,A_n^{l-1}]$和 $[R_1^{l-1},\ldots,R_n^{l-1}]$。

用户依次更新其排名 $l=1\ldots L$。当轮到用户 u_l时，u_l 首先向多方计算服务器请求当前差值向量 $\mathbf{A}^{l-1}-\mathbf{R}^{l-1}$，促使多方计算服务器根据其本地的 $\mathbf{A}^{l-1}$ 和 $\mathbf{R}^{l-1}$ 秘密份额，计算出 $\mathbf{A}[\![\mathbf{R}^{l-1}]\!]$ 的秘密共享（获取不公平性度量过程）。原则上，每个多方计算服务器都可以将 $\mathbf{A}^{l-1}-\mathbf{R}^{l-1}$ 的秘密份额发送给用户 u_l，由 u_l 将这些份额合并，以构造 $\mathbf{A}^{l-1}-\mathbf{R}^{l-1}$ 的值。然而，尽管 $\mathbf{A}^{l-1}-\mathbf{R}^{l-1}$ 仅由聚合信息构成，这个值仍可能向用户 u_l泄露关于先前用户 u_1、.....、u_{l-1}的信息，尤其是在 u_l 是最先进行重排序的用户之一时。在我们的方案中，多方计算服务器会在将结果发送给用户 u_l 之前，对 $[\![\mathbf{A}^{l-1}-\mathbf{R}^{l-1}]\!]$ 各个索引处的值添加拉普拉斯噪声，以缓解这种隐私损失（获取不公平性度量过程）。我们将这种经过扰动的秘密共享记为 $[\![\xi]\!]$。多方计算服务器以这种方式提供的差分隐私保证是：返回 ξ 任一特定值的概率，与在计算 $[\![\mathbf{A}^{l-1}-\mathbf{R}^{l-1}]\!]$ 时不纳入先前用户 u_i（$i=1\ldots l-1$）的数据而返回该值的概率非常接近（参见公式6）。这意味着，返回给用户 u_l 的 ξ 值不会泄露在轮到 u_l之前已完成重排序的用户的信息。为此，多方计算服务器

使用用于从拉普拉斯分布中进行安全采样的 MPC 协议 π_{LAP} 生成拉普拉斯噪声的秘密份额（如 Pentyala 等人 [20] 所述），并将这些秘密份额加到 $[\![\mathbf{A}^{l-1} - \mathbf{R}^{l-1}]\!]$上，从而有效模拟全局差分隐私范式，而无需依赖中心化可信聚合器。下文将进一步介绍拉普拉斯噪声的尺度参数 b 。

算法 1 保护隐私的公平项目排序

在 L 位用户中私密地实现 EOAA
每个排名中的$n \leftarrow$ 个项目数
要重排序的$L \leftarrow$ 个排名数
k 质量约束中的$\leftarrow$ 个项目数
公式 3
$\mathbf{w} \leftarrow$ 注意力权重
$\hat{}\mathbf{w} \leftarrow$归一化$(\mathbf{w})$
初始化()
对于每个 u_l, **其中** $l = 1 \ldots L$ **执行**
$[\![\boldsymbol{\xi}]\!] \leftarrow$ 获取不公平性度量()
$[\![\hat{}\mathbf{w}^*]\!], [\![\hat{}\mathbf{r}]\!] \leftarrow$ 重排序$([\![\boldsymbol{\xi}]\!], u_l, k)$
更新聚合$([\![\hat{}\mathbf{w}^*]\!], [\![\hat{}\mathbf{r}]\!])$
结束循环

用户 u_l 子程序
过程 重排序$([\![\boldsymbol{\xi}]\!], u_l, k)$
$\boldsymbol{\xi} \leftarrow (\epsilon/L) \sum [\![\boldsymbol{\xi}]\!]$
$\mathbf{r} \leftarrow \mathcal{M}(u_l, \cdot, \mathcal{D})$
$\hat{}\mathbf{r} \leftarrow$归一化$(\mathbf{r})$
$\mathbf{s} \leftarrow$ 整数线性规划$(\boldsymbol{\xi}, \hat{}\mathbf{r}\ k)$
$\hat{}\mathbf{w}^* \leftarrow \hat{}\mathbf{w}[\mathbf{s}]$
返回 $[\![\hat{}\mathbf{w}^*]\!], [\![\hat{}\mathbf{r}]\!]$
结束过程

多方计算服务器的子程序
过程 初始化()
$\Delta f \leftarrow$根据公式 11 计算的敏感度
$\epsilon \leftarrow$ 隐私预算
$[\![\mathbf{A}]\!] \leftarrow [\![0]\!]$
$[\![\mathbf{R}]\!] \leftarrow [\![0]\!]$
结束过程

过程获取不公平性度量()
//用于全局差分隐私的安全多方计算协议
$b \leftarrow \Delta f/(\epsilon/(n \cdot L))$
$[\![\boldsymbol{\xi}]\!] \leftarrow [\![\mathbf{A} - \mathbf{R}]\!] + \pi_{\mathsf{LAP}}(b)$
返回 $[\![\boldsymbol{\xi}]\!]$
结束过程

过程 更新聚合$([\![\hat{}\mathbf{w}^*]\!], [\![\hat{}\mathbf{r}]\!])$
//执行聚合的 MPC 协议
$[\![\mathbf{A}]\!] \leftarrow [\![\mathbf{A}]\!] + [\![\hat{}\mathbf{w}^*]\!]$
$[\![\mathbf{R}]\!] \leftarrow [\![\mathbf{R}]\!] + [\![\hat{}\mathbf{r}]\!]$
结束过程

一旦用户 u_l 从每个多方计算服务器接收到 $\boldsymbol{\xi}$ 的秘密份额， u_l 便可将这些秘密份额相加以获得 $\mathrm{A}^{l-1} - \mathrm{R}^{l-1} + \pi_{\mathsf{LAP}}(b)$，并将其作为 $\mathrm{A}^{l-1} - \mathrm{R}^{l-1}$ 的代理值，随后针对 $X_{i,\ j}$（$i = 1 \ldots n$ 和 $j = 1 \ldots n$）求解第 2.1 节中的整数线性规划程序（重排序过程）。在我们的实现中，我们将 $\mathrm{A}^{l-1} - \mathrm{R}^{l-1} + \pi_{\mathsf{LAP}}(b)$ 乘以一个正因子 ϵ/L，以便更容易计算整数线性规划的解。需要注意的是，乘以正因子不会影响 $X_{i,\ j}$ 中的结果。随后，$X_{i,\ j}$ 可转换为一个索引向量 s，用于按照 s 的顺序重新排列归一化注意力权重 $\hat{}\mathrm{w}$。$\hat{}\mathrm{w}^*$ 是在 s 的顺序中分配给每个索引处项目的注意力权重向量。因此，$\hat{}\mathrm{w}^*$ 和 $\hat{}\mathrm{r}$ 构成重排序ρ_l^*。用户 u_l 随后通过将这些向量中的值拆分为秘密份额 $[\![\hat{}\mathrm{w}^*]\!]$ 和 $[\![\hat{}\mathrm{r}]\!]$, 来对其加密，并将这些份额分发给多方计算服务器。这使得多方计算服务器能够将其聚合值的秘密份额更新为 $[\![\mathrm{A}^l]\!]$ 和 $[\![\mathrm{R}^l]\!]$（更新聚合过程），以便在下一位用户 u_{l+1}发出请求时使用。整个过程会重复进行，直到所有用户均完成其重排序。

尺度参数 b。为了使我们的算法满足 ϵ-差分隐私，多方计算服务器通过向真实聚合值添加噪声来回答每个查询。为此，多方计算服务器从均值为 0、尺度为 $b = \Delta f/\epsilon'$ 的拉普拉斯分布中采样噪声

其中 Δf 表示敏感度， ϵ' 表示每次查询的隐私预算。下一节将介绍这些参数的适当取值。在算法 1 中，每个用户 u_l（$l = 1 \dots L$）通过获取不公平性度量过程向多方计算服务器查询关于每个项目 $A_i^{l-1} - R_i^{l-1}$（d_i）的聚合信息 $i = 1 \dots n$。多方计算服务器需要回答的查询总数换言之为$n \cdot L$。这些查询针对存在重叠的数据集执行，因为 u_l 查询用户 u_1、.....、u_{l-1}的聚合信息； u_{l+1} 查询用户 u_1、.....、u_l的聚合信息，依此类推。给定总隐私预算 ϵ，因此我们为每次查询分配 $\epsilon' = \epsilon /$（$n \cdot L$）。

Δf 是针对聚合值 ${A_i}^{l-1} - {R_i}^{l-1}$计算的敏感度，由公式 11 给出。公式 11 计算的是任意单个用户对该聚合值所能贡献的最大值。

$$\hat{r}_{\min} = \frac{r_{\min} - r_{\min}}{r_{\max} - r_{\min}} \Bigg/ \left(\frac{r_{\min} - r_{\min}}{r_{\max} - r_{\min}} + (n-1) \left(\frac{r_{\max} - r_{\min}}{r_{\max} - r_{\min}} \right) \right) = 0 \tag{7}$$

$$\hat{r}_{\max} = \frac{r_{\max} - r_{\min}}{r_{\max} - r_{\min}} \Bigg/ \left(\frac{r_{\max} - r_{\min}}{r_{\max} - r_{\min}} + (n-1) \left(\frac{r_{\min} - r_{\min}}{r_{\max} - r_{\min}} \right) \right) = 1 \tag{8}$$

$$\hat{w}_{\min} = \frac{w_n}{\sum_{j=1}^{n} w_j} \tag{9}$$

$$\hat{w}_{\max} = \frac{w_1}{\sum_{j=1}^{n} w_j} \tag{10}$$

$$\Delta f = \max(|\hat{w}_{\max} - \hat{r}_{\min}|, |\hat{w}_{\min} - \hat{r}_{\max}|) \tag{11}$$

公式 9、10 基于归一化几何注意力模型，公式 7、8 则基于多方计算服务器可能接收到的归一化相关性分数的范围。 Δf 和 b 的计算独立于用户数据，因此可以由其中一台多方计算服务器在明文状态下预先计算，即无需加密（参见初始化过程）。

5 结果

5.1 数据集

我们的实验使用了三个推荐系统数据集：亚马逊数字音乐、[8] Book Crossing、[9] 和 MovieLens-1M。[10] 每个数据集都包含有关用户和项目的信息，以及用户对项目给出的评分。表 1 详细列出了每个数据集的用户数、项目数、评分数以及可能评分的范围。

5.2 实验设置

我们为每个数据集训练了一个奇异值分解（SVD）模型[11] ，并预测了每个用户-物品对的相关性分数。我们假设这些模型

[8] http://jmcauley.ucsd.edu/data/amazon/links.html[9]
http://www2.informatik.uni-freiburg.de/~cziegler/BX/[10]
https://grouplens.org/datasets/movielens/1m/[11]
https://surpriselib.com/

表 1：用于训练各 SVD 模型的数据集统计信息

数据集	用户数	项目数	评分数	评分等级
亚马逊数字音乐	478，235	266，414	836，006	1、2、.....5
Book Crossing	77，805	185，973	433，671	1，2，.....10
MovieLens 1M	6，040	3、706	1，000，209	1，2，...，5

是在保护隐私的方式下训练的。在实验中，我们为所有数据集选择$n = 100$ 个项目进行重排序，并对亚马逊数字音乐和 Book Crossing 数据集中的 $L = 3000$ 个用户的排名进行重排序，同时对 MovieLens-1M 数据集中的所有 $L = 6040$ 个用户的排名进行重排序。我们使用 Gurobi[12] 求解公式 2–4 中的整数线性规划。我们将质量损失约束设为 $k = 100$, 并根据公式 11 计算敏感度，所有数据集的敏感度均为 $\Delta f = 1$ 。我们针对隐私预算 $\epsilon \in \{0.5, 1, 10, 100, 1000, 10000, 100000\}$进行了实证分析。

所有安全多方计算均在 MP-SPDZ 框架中完成 [15]，并在一个环 $\mathbb{Z}_q$ 上执行，其中包含 $q = 2^{64}$。我们在恶意多数安全设置下进行实验，采用 2 个计算参与方（两方计算）和被动对手。

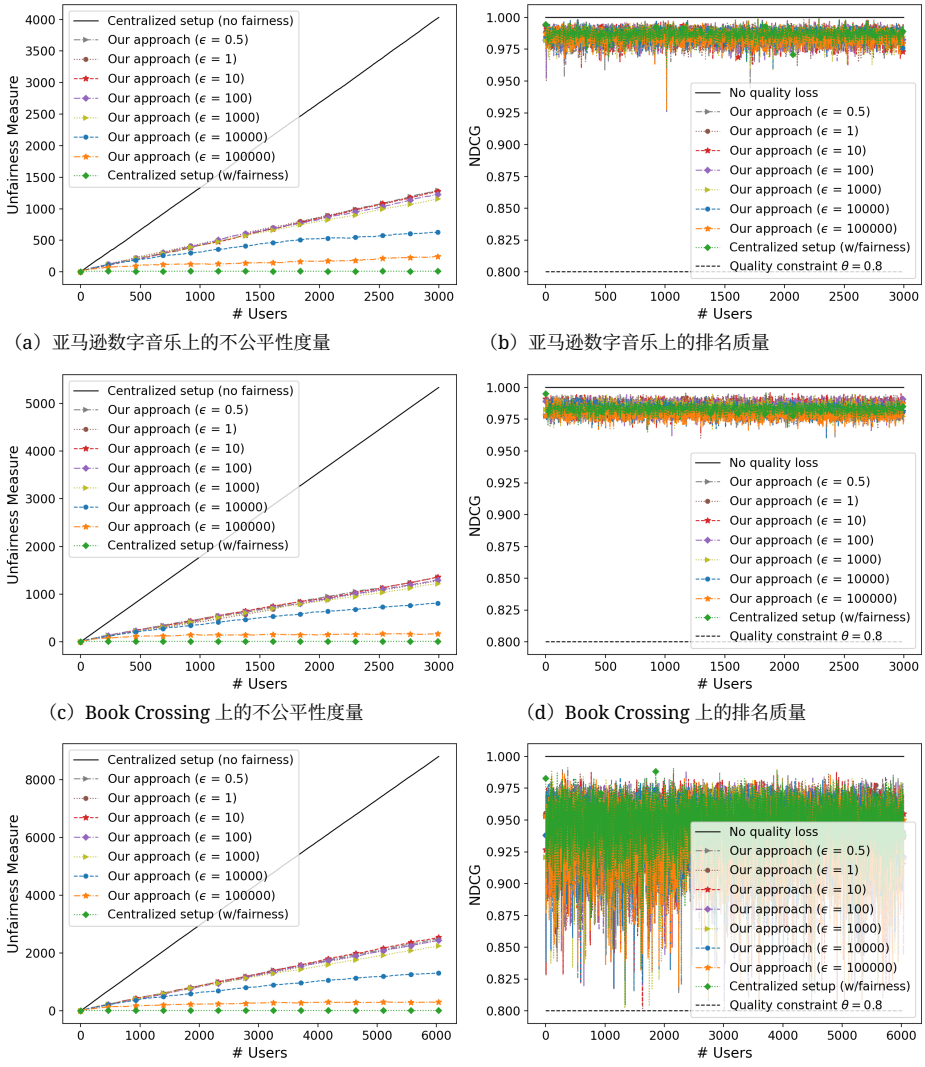
我们根据不公平性（公式 1）和效用（公式 5）评估我们的方法，并研究隐私、公平性与效用之间的权衡。

5.3 讨论

公平性与隐私权衡 图 2（左列；图 2a、2c 和 2e）展示了在保护用户隐私时项目公平性所付出的代价。“集中式设置（无公平性）”表示未采取任何偏差缓解措施时的不公平性度量，“集中式设置（有公平性）”表示在集中式设置中应用第 2.1 节的后处理技术、且不提供任何隐私保护时的不公平性度量。理想情况下，我们需要采用隐私保护技术，使不公平性度量接近“集中式设置（有公平性）”的结果。结果表明，即使采用隐私保护技术，我们的方法仍能提升公平性。具体而言，我们的方法在流程的每一步都能保护用户隐私，包括用户向服务器传输 $[\![\hat{\mathbf{w}}^*]\!]$ 和 $[\![\hat{\mathbf{r}}]\!]$ 时，以及服务器向用户传输 $[\![\boldsymbol{\xi}]\!]$ 时。我们的结果显示，隐私与不公平性之间存在权衡：隐私预算降低（即隐私保护增强）会使公平性付出更高代价，这与现有文献的结论一致。这是因为所添加的噪声会扰动不公平性度量的值，进而影响整数线性规划相较于不采用差分隐私的集中式设置计算重新排名的效果。值得注意的是，即使 ϵ 较高，我们的方案仍能保护输入隐私。

效用与隐私权衡 图 2（右列；图 2b、图 2d 和图 2f）展示了为用户引入隐私保护对重排序质量的影响。

[12] https://www.gurobi.com/



（a）亚马逊数字音乐上的不公平性度量

（b）亚马逊数字音乐上的排名质量

（c）Book Crossing 上的不公平性度量

（d）Book Crossing 上的排名质量

（e）MovieLens-1M 上的不公平性度量

（f）MovieLens-1M 上的排序质量

图 2：模型在各数据集上的性能

）。归一化折扣累计增益 $= 1$ 表示归一化折扣累计增益的上限，表明与原始排名相比，项目相关性分数的排序没有变化。归一化折扣累计增益 $= 0.8$ 处的虚线表示整数线性规划中设定的质量约束θ。结果表明，无论为保护隐私而添加的噪声量是多少，重新排名的质量始终保持在设定的边界 $0.8 \leq$ 归一化折扣累计增益 ≤ 1内。我们的研究表明，使用我们的方法，可以保护用户隐私，同时不会使效用损失超过阈值 θ

最初在整数线性规划中设定。

由此产生的隐私–公平性权衡源于对输出隐私的保护。无论是否保护隐私，效用–公平性权衡都源于偏差缓解技术。

运行时间 所有实验均在一台配备 16 GB 内存的 2.6 GHz 六核英特尔酷睿 i7 上进行。在集中式设置下，为 $n = 100$ 对单个用户的排名进行重排序，耗时约 0.67 秒（对 $L = 6{,}040$ 位用户取平均值）。在采用混合电路 [10]的两方计算被动安全设置中，增加隐私保护所带来的额外运行时间成本不到每位客户端 5 秒。不同安全设置下的运行时间各不相同。在三方计算被动安全设置 [2], 下，这项额外运行时间可缩短至不到 1 秒。我们认为，为用户排名进行重排序所增加的运行时间成本，值得以隐私保护方面的收益来换取。值得注意的是，多方计算方案通常分为两个阶段：离线阶段和在线阶段；我们报告了这两个阶段的运行时间。离线阶段执行与数据无关的计算，因此可以在用户重新排名之前完成。这样可以进一步提升我们方法的响应速度，使其在实践中可行，并接近实时。

6 结论与未来工作

我们提出了一种新颖的理念：在推荐生态系统中采用后处理技术，在保护消费者（用户）隐私的同时，促进生产者（项目）公平性。我们提出了一种方法，让用户与安全多方计算（MPC）服务器协同工作，根据相关性分数和注意力权重对项目进行重排序。MPC 服务器仅接收加密形式（秘密份额）的用户数据，并在数据保持加密的状态下完成所有计算。此外，每当 MPC 服务器需要向用户发布聚合信息时，都会向其中加入噪声，以提供差分隐私（DP）保障，从而避免向其他用户泄露任何用户的数据。

我们通过与集中式方法进行比较，证明采用我们提出的隐私保护方法能够缓解不公平性，且不会额外损害效用；在集中式方法中，所有用户都会向中央服务器披露其数据。我们的方法可以扩展至其他偏差缓解技术，以及排名公平性的多种其他概念。我们相信，这项工作将推动隐私与推荐系统公平性交叉领域的研究，并鼓励开发面向多利益相关者推荐系统中生产者和消费者的端到端隐私保护与公平性促进流程。

致谢本项目部分由加拿大高等研究院（CIFAR）资助。

参考资料

1. Ammad-Ud-Din, M., Ivannikova, E., Khan, S.A., Oyomno, W., Fu, Q., Tan, K.E., Flanagan, A.: 用于隐私保护个性化推荐系统的联邦协同过滤。arXiv预印本 arXiv:1901.09888（2019） 2. Araki, T., Furukawa, J., Lindell, Y., Nof, A., Ohara, K.: 具有诚实多数的高吞吐量半诚实安全三方计算。载于：ACM SIGSAC计算机与通信安全会议。第805–817页（2016） 3. Biega, A.J., Gummadi, K.P., Weikum, G.: 注意力公平性：通过摊销实现排名中的个体公平性。载于：第41届国际ACM SIGIR信息检索研究与发展会议。第405–414页（2018） 4. Canny, J.: 保护隐私的协同过滤。载于：IEEE安全与隐私研讨会。第45–57页（2002） 5. Celis, L.E., Straszak, D., Vishnoi, N.K.: 带公平性约束的排序。载于：第45届国际自动机、语言与程序设计研讨会（ICALP 2018）。莱布尼茨国际信息学论文集（LIPIcs），第107卷，第28:1–28:15页（2018） 6. Chai, D., Wang, L., Chen, K., Yang, Q.: 安全联邦矩阵分解。《IEEE智能系统》**36**(5)，11–20（2020） 7. Cramer, R., Damgard, I., Nielsen, J.: 安全多方计算与秘密共享。剑桥大学出版社印刷版，纽约（2015） 8. Dehghani, M., Azarbonyad, H., Kamps, J., de Rijke, M.: 分享模型而非数据：用于排序的隐私保护模仿学习。arXiv预印本 arXiv:1707.07605（2017） 9. Dwork, C., Roth, A.: 差分隐私的算法基础。《理论计算机科学基础与趋势》**9**(3-4)，211–407（2014） 10. Escudero, D., Ghosh, S., Keller, M., Rachuri, R., Scholl, P.: 面向混合算术-二进制电路的改进型安全多方计算基本工具。载于：国际密码学年度会议。第823–852页。施普林格（2020） 11. Ge, Z., Liu, X., Li, Q., Li, Y., Guo, D.: PrivItem2Vec：一种用于Top-N推荐的隐私保护算法。《国际分布式传感器网络杂志》**17**(12)（2021） 12. Joachims, T., Granka, L., Pan, B., Hembrooke, H., Radlinski, F., Gay, G.: 评估网络搜索中点击和查询改写所产生的隐式反馈的准确性。《ACM信息系统汇刊》（TOIS）**25**(2)，7–es（2007） 13. Joachims, T., Radlinski, F.: 从隐式反馈中学习的搜索引擎。《计算机》**40**(8)，34–40（2007） 14. Kay, M., Matuszek, C., Munson, S.A.: 职业图像搜索结果中的代表性不平等与性别刻板印象。载于：第33届ACM计算系统中的人为因素年度会议论文集。第3819–3828页（2015） 15. Keller, M.: MP-SPDZ：一个通用的多方计算框架。载于：2020年ACM SIGSAC计算机与通信安全会议论文集。第1575–1590页（2020） 16. Kharitonov, E.: 基于进化策略的联邦在线学习排序。载于：第12届ACM网络搜索与数据挖掘国际会议论文集。第249–257页（2019） 17. Liu, Y., Ge, K., Zhang, X., Lin, L.: 面向推荐系统的实时注意力相似用户模型。载于：第25届ACM SIGKDD知识发现与数据挖掘国际会议论文集。第2765–2773页（2019）

18. Mehrotra, R., McInerney, J., Bouchard, H., Lalmas, M., Diaz, F.: 迈向公平市场：推荐系统中相关性、公平性与满意度之间权衡的反事实评估。载于：第27届ACM信息与知识管理国际会议论文集。第2243–2251页（2018） 19. Morik, M., Singh, A., Hong, J., Joachims, T.: 动态学习排序中的公平性与偏差控制。载于：第43届国际ACM SIGIR信息检索研究与发展会议论文集。第429–438页（2020） 20. Pentyala, S., Neophytou, N., Nascimento, A., De Cock, M., Farnadi, G.: 跨设备联邦学习中的隐私保护群体公平性。载于：NeurIPS因果与隐私视角下的算法公平性研讨会论文集，机器学习研究论文集（2023） 21. Resheff, Y.S., Elazar, Y., Shahar, M., Shalom, O.S.: 通过对用户表示进行对抗训练，实现推荐系统中的隐私与公平性。arXiv预印本 arXiv:1807.03521（2018） 22. Sapiezynski, P., Zeng, W., E Robertson, R., Mislove, A., Wilson, C.: 量化用户注意力对排序列表中群体公平代表性的影响。载于：2019年万维网大会伴随论文集。第553–562页（2019） 23. Sato, R.: 隐私推荐系统：用户如何在没有日志数据的情况下构建自己的公平推荐系统？载于：2022年SIAM国际数据挖掘会议（SDM）论文集。第549–557页。SIAM（2022） 24. Singh, A., Joachims, T.: 排名中的曝光公平性。载于：第24届ACM SIGKDD知识发现与数据挖掘国际会议论文集。第2219–2228页（2018） 25. Singh, A., Joachims, T.: 排序公平性的策略学习。《神经信息处理系统进展》**32**（2019） 26. Wang, S., Liu, B., Zhuang, S., Zuccon, G.: 高效且保护隐私的联邦在线学习排序。载于：2021年ACM SIGIR信息检索理论国际会议论文集。第3–12页（2021） 27. Wang, S., Zhuang, S., Zuccon, G.: 使用进化策略的联邦在线学习排序：一项可复现性研究。载于：欧洲信息检索会议。第134–149页。施普林格（2021） 28. Wu, C., Wu, F., Cao, Y., Huang, Y., Xie, X.: FedGNN：用于隐私保护推荐的联邦图神经网络。arXiv预印本 arXiv:2102.04925（2021） 29. Yang, D., Qu, B., Cudré-Mauroux, P.: 面向基于排序的个性化推荐的隐私保护社交媒体数据发布。《IEEE知识与数据工程汇刊》**31**(3)，507–520（2018） 30. Yang, K., Stoyanovich, J.: 衡量排序输出的公平性。载于：第29届科学与统计数据库管理国际会议论文集。第1–6页（2017） 31. Zehlike, M., Bonchi, F., Castillo, C., Hajian, S., Megahed, M., Baeza-Yates, R.: Fa* ir：一种公平 top-k 排序算法。载于：2017年ACM信息与知识管理会议论文集。第1569–1578页（2017）