arXiv:2304.01541v1 [stat.ML] 4 Apr 2023

通过压缩实现隐私放大：实现分布式均值估计中最优的隐私-准确率-通信权衡

Wei-Ning Chen† Dan Song† Ayfer ¨Ozg¨ur† Peter Kairouz‡

斯坦福大学†，Google Research‡

摘要

隐私与通信约束是联邦学习（FL）和分析（FA）面临的两大主要瓶颈。我们研究联合通信约束与（ε, δ）差分隐私（DP）约束下均值估计和频率估计（分别是 FL 和 FA 的典型模型）的最优准确度。我们同时考虑中心化差分隐私模型和多消息洗牌差分隐私模型。我们证明，为了在（ε，δ）差分隐私下实现最优 ℓ_2 误差，每个客户端只需向服务器发送 $\Theta\left(n\min\left(\varepsilon,\ \varepsilon^2\right)\right)$ 比特（用于 FL），以及 $\Theta\left(\log\left(n\min\left(\varepsilon,\ \varepsilon^2\right)\right)\right)$ 比特（用于 FA），其中 n 为参与客户端的数量。若不进行压缩，均值估计和频率估计问题中每个客户端分别需要发送 $O(d)$ 比特和 $O(\log d)$ 比特（其中 d 对应于 FL 中的可训练参数数量或 FA 中的域大小），这意味着在 $n\min\left(\varepsilon,\ \varepsilon^2\right) = o(d)$ 的情形下可以节省大量通信开销，而这通常正是实践中相关的情形。

我们提出两种利用压缩实现隐私放大并达到隐私、通信与准确度之间最优权衡的方法。在这两种方法中，每个客户端仅传输其样本的部分信息；我们证明，通过随机选择每个客户端贡献的部分信息，可以放大隐私。在第一种方法中，随机选择结果会告知服务器，因此能够实现中心化差分隐私保证，并达到隐私、通信与准确度之间的最优权衡。在第二种方法中，每个客户端对随机选取的数据部分进行本地隐私化，再由安全洗牌器将其匿名化，从而无需可信服务器。这种方法构成了一种多消息洗牌方案，也能达到相同的最优权衡。因此，本文确立了中心化差分隐私框架和多消息洗牌框架下，隐私、通信与准确度三者之间的最优权衡。[1]

1 引言

在联邦学习（FL） [67, 63, 60] 和分析（FA）的基本设定中，服务器希望对保存在客户端设备上的原始数据执行特定的学习或分析任务。例如，联邦学习中的模型更新或联邦分析中的直方图估计，都可以建模为分布式均值估计问题。解决该问题的方法是让客户端向服务器传输针对性消息。服务器在发布计算所得的均值之前向其中注入噪声，以确保用户数据的隐私（通过明确的差分隐私（DP） [38] 保证来界定）；例如，服务器可以计算平均模型更新，并通过添加噪声对其进行扰动。这称为可信服务器模型或中心化差分隐私模型，因为该模型将隐私化工作交由中央服务器负责；这是当今实现联邦学习和分析最常见的方式之一 [2]。

本文首先针对中心化差分隐私设定下的分布式均值估计提出以下问题：既然服务器只需发布均值的一个带噪版本，或者说近似版本，客户端能否向服务器传输“更少的信息”？更具体地说，在给定所需隐私级别的情况下，能否在不牺牲准确度的前提下降低网络的通信负载，也就是说，保持

[1]本文中最优性的概念是阶数意义上的，且在某些情况下存在对数因子差距。具体表述请参见结果部分。[2]我们假设存在一位会忠实执行差分隐私机制的可信服务提供商。可以通过在可远程验证的可信执行环境 [11]中实现差分隐私机制来确保这一点。

所需隐私级别下相同的（阶数意义上最优的）准确度？近年来，人们对中心化差分隐私模型 [1] 以及不同模型下联邦学习和联邦分析的通信效率与隐私问题投入了大量关注，包括本地差分隐私 [77, 62, 57, 79, 17, 6, 16, 32]，洗牌 [40, 43] 和分布式差分隐私[9, 58, 8, 33, 34]；然而，这个基本问题似乎仍未得到解答。

客户端可以只向服务器传输有关其样本的部分信息，从而降低通信负载。例如，在模型更新场景中，每个客户端可以只更新部分模型系数。在直方图估计场景中，客户端样本的信息可以被“拆分”为多个部分，客户端只需传输其中一部分。然而，这意味着服务器收集到的信息更少，或者说用于估计目标量的样本实际上更少。例如，在前述模型更新场景中，每个模型系数只由部分客户端更新。简单计算即可发现，这会增加估计值对每个用户样本的敏感度，因此，为了达到相同的隐私级别，服务器需要添加更多噪声，从而降低准确度。

我们通过一个简单但富有启发性的观察绕过这一难题：当每个客户端只传输其样本的部分信息时，我们可以随机选择每个客户端贡献的部分，从而实现隐私放大。只能访问服务器所公布最终估计值的下游模块，并不知道每个客户端分别贡献了哪一部分，因此实现了隐私放大。此前文献已研究通过子采样实现的隐私放大 [65, 14] ，但通常只讨论服务器从可用客户端池中随机选择一部分客户端时的隐私放大。与此不同，在我们的场景中，随机性融入了每个客户端的压缩方案，所涉及的是每个客户端传输的信息片段，而非参与客户端的选择。我们将这种增益称为通过压缩实现隐私放大，并利用它确立中心化差分隐私模型下最优的通信负载—隐私—准确度权衡。请注意，在本地差分隐私模型中无法利用这种增益，因为服务器并不可信，而且知道每条消息及其对应的客户端身份。事实上，已知本地差分隐私模型中的隐私—准确度权衡明显劣于中心化差分隐私模型（见表 1）。

这自然引出了一个后续问题：我们能否利用通过压缩实现的隐私放大，并在安全聚合 [33] 和洗牌 [40] 类型的模型中实现同样的三方权衡？对于安全聚合，答案是否定的。文献[31] 研究了安全聚合的通信开销，其开销显著高于本文所确立的中心化差分隐私通信开销（见表 1）。另一方面，洗牌的通信开销仍是一个尚未解决的问题，正如文献[31]所述。我们通过证明多消息洗牌方案也能实现最优的中心化差分隐私权衡，解决了这一开放问题；这也确立了多消息洗牌方案的最优通信开销。和之前一样，我们的方案利用了类似的隐私放大增益。每个客户端传输其样本的部分信息；安全洗牌器会抹去消息的身份，因此不可信的服务器无法得知每个客户端分别贡献了哪一部分信息。然而，要实现最优权衡，关键在于每个客户端将其信息拆分为多条消息，并通过在不同轮次之间仔细分配隐私预算来采用多轮洗牌。相比之下，安全聚合无法利用类似的增益，因为安全聚合的线性性要求所有参与的客户端传输一致的信息（相同的部分），从而排除了通过压缩实现隐私放大的可能。详细比较见表 1。

我们的贡献。 我们将分布式均值和频率估计视为 FL 和 FA 的典型构件。我们同时研究中心化差分隐私模型和多消息洗牌模型。我们刻画了分布式均值估计中阶最优的隐私-准确率-通信权衡，并为中心化差分隐私模型下的频率估计提供了一种可实现的方案。我们的结果表明，无需牺牲额外的准确度，也可以同时实现隐私保护和通信效率。特别地，我们证明，对于均值估计和频率估计，在（ε，δ）-隐私下，$\tilde{O}\left(n\min\left(\varepsilon,\ \varepsilon^2\right)\right)$ 以及 $\tilde{O}\left(\log\ \left(n\min\left(\varepsilon,\ \varepsilon^2\right)\right)\right)$ 比特的（每客户端）通信量足以达到阶最优误差，其中 n 为参与客户端的数量。在不进行压缩的情况下，对于均值估计和频率估计问题，每个客户端分别需要 $O(d)$ 比特和 $\log d$ 比特（其中，d 是 FL 中可训练参数的数量，或 FA 中的域大小），这意味着在 $n\varepsilon^2 = o(d)$ 的情形下可以显著节省通信开销（假设 $\varepsilon = O(1)$）。我们注意到，这不仅是跨机构 FL/FA 中的相关情形，也是跨设备 FL/FA 中的相关情形。例如，在实际的 FL 中，d 通常介于 10^6–10^9, 之间，而 n（每轮次 的样本量）通常要小得多（例如，数量级为 10^3–10^5）。对于分布式均值估计，

	通信（比特）	ℓ_2 误差
本地差分隐私 [32, 42]	$\Theta(\lceil\varepsilon\rceil)$	$\Theta\left(\frac{d}{n^2 \min(\varepsilon^2,\varepsilon)}\right)$
分布式差分隐私（采用安全聚合） [33]	$\tilde{O}\left(n^2 \min\left(\varepsilon, \varepsilon^2\right)\right)$	$O\left(\frac{d}{d \log n^2 \varepsilon^2 \min(\varepsilon,\varepsilon)}\right)$
中心化差分隐私（定理 4.4）	$\tilde{O}\left(n \min\left(\varepsilon, \varepsilon^2\right)\right)$	$O\left(\frac{d}{n^2 \min(\varepsilon^2,\varepsilon)}\right)$
洗牌差分隐私（定理 6.4）	$\tilde{O}\left(n \log(d) \min\left(\varepsilon, \varepsilon^2\right)\right)$	

表 1：本地、分布式、中心化和洗牌差分隐私下 ℓ_2 均值估计的通信开销比较（其中 δ 项已隐藏）。与本地差分隐私相比，我们看到中心化差分隐私下的误差衰减快得多（例如， $1/n^2$ 而非 $1/n$）；与采用安全聚合的分布式差分隐私相比，我们的方案达到相近的准确度，同时将通信开销降低了 n倍。

我们表明，中心化差分隐私权衡也可以通过多消息洗牌方案实现（通信开销仅相差一个 $\log d$ 因子）。因此，本文为中心化差分隐私和多消息洗牌框架建立了隐私、通信与准确度之间的三方权衡，而这两个问题在此前的文献中都属于开放问题。与本地差分隐私相比，在 $\varepsilon = O(1)$ 时只需 1 比特即可实现，这表明中心化／洗牌差分隐私具有更高的通信开销，但能够实现小得多的误差（相差 n 倍），因此在实际应用中通常更具优势。与分布式差分隐私相比，在后者中，服务器通过安全多方计算（例如， [23, 8, 34]）聚合本地（编码后的）消息；我们可以将通信开销降低 n 倍，从而表明借助可信服务器或洗牌器可以降低通信开销。我们在表 1 中总结了本文主要结果与本地差分隐私和分布式差分隐私的比较。

记号。 本文中，对于任意 $m \in \mathbb{N}$，我们用 $[m]$ 表示 $\{1, ..., m\}$ 的集合。随机变量（向量）(X_1、.....、X_m)记作 X^m。我们还使用巴赫曼–朗道渐近记号，即 O， o， Ω ω，以及 Θ。

2 问题表述

我们首先介绍差分隐私下的分布式均值估计（DME） [73] 问题。请注意，DME 与采用随机梯度下降（SGD）（或类似随机优化方法，例如 FedAvg [67]）的联邦学习密切相关；在每次迭代中，服务器通过本地模型更新的带噪均值来更新全局模型。该带噪估计通常通过分布式均值估计方案获得，因此可以轻松地基于差分隐私分布式均值估计方案构建分布式差分隐私随机梯度下降方案（进而构建隐私保护联邦学习方案）。此外，如 [49], 所示，只要我们在每一轮都能获得梯度的无偏估计，SGD（或差分隐私随机梯度下降）的收敛速率就取决于 ℓ_2 估计误差。

分布式均值估计。设有 n 个客户端，每个客户端都拥有满足 $\|x_i\|_2 \leq C$ 的本地数据 $x_i \in \mathbb{R}^d$，其中 $C > 0$ 是某个常数（可以将 x_i 视为裁剪后的本地梯度）。服务器希望在与这些 n 个客户端通信后，利用 $x^n = (x_1、...、x_n)$ 得到均值 $\mu(x^n) \triangleq \frac{1}{n}\sum_i x_i$ 的估计值 $\hat{}\mu$。为此，每个客户端在本地将 x_i 压缩为一条 b 位消息 $Y_i = \mathsf{enc}_i(x_i) \in \mathcal{Y}$，压缩过程通过本地编码器 enc_i：$\mathcal{X} \mapsto \mathcal{Y}$（其中 $|\mathcal{Y}| \leq 2^b$），随后将消息发送给中央服务器。服务器收到 $Y^n = (Y_1、.....、Y_n)$ 后，计算估计值 $\hat{}\mu = \mathsf{dec}(Y^n)$，使其满足以下差分隐私要求：

定义 2.1（差分隐私）。 机制 $\hat{}\mu$ 是 (ε, δ)-差分隐私的，当对于任意相邻数据集 $x^n := (x_1, ..., x_i, ..., x_n)$、$x'^n := (x_1, ..., x'_i, ..., x_n)$，以及可测 $\mathcal{S} \subseteq \mathcal{Y}$，

$$\Pr\{\hat{\mu} \in \mathcal{S} | x^n\} \leq e^{\varepsilon} \cdot \Pr\{\hat{\mu} \in \mathcal{S} | x'^n\} + \delta,$$

其中概率是针对 $\hat{}\mu$ 的随机性而言的。

我们的目标是设计能够最小化 ℓ_2^2 估计误差的方案：

$$\min_{(\mathsf{enc}_1(\cdot),...,\mathsf{enc}_n(\cdot),\mathsf{dec}(\cdot))} \max_{x^n} \mathbb{E}\left[\|\hat{\mu}(\mathsf{enc}_1(x_1), ..., \mathsf{enc}_n(x_n)) - \mu(x^n)\|_2^2\right],$$

受限于 b 位通信和 $(\varepsilon,\ \delta)$-差分隐私约束。

分布式频率估计。同样，频率估计也可以表述为一个均值估计问题，但使用的是稀疏（独热）向量。设每个用户 i 持有一个取值域 $\mathcal{X}$大小为 d 的域 x_i 中的项 x_i。服务器旨在估计这些 n 项的直方图。不失一般性，我们可以假设 $\mathcal{X}:=\{e_1,...,e_d\}\in\{0,1\}^d$（其中 e_j 是 $\mathbb{R}^d$中的第 j 个标准基向量），也就是说，每个项都表示为一个独热向量。然后，这些 n 项的直方图可表示为 $\pi(x^n):=\sum_{i\in[n]}x_i$。与均值估计问题类似，客户端在本地计算后发送 $Y_i=\mathsf{enc}_i(x_i)\in\mathcal{Y}$（对于某个满足$|\mathcal{Y}|\leq 2^b$的 $\mathcal{Y}$），中央服务器则计算估计值 $\hat{}\pi=\mathsf{dec}\left(Y^n\right)$。我们的目标是设计能够最小化 ℓ_2^2 或 ℓ_1 误差[3]的方案：

$$\min_{(\mathsf{enc}_1(\cdot),\ldots,\mathsf{enc}_n(\cdot),\mathsf{dec}(\cdot))}\max_{x^n}\mathbb{E}\left[\left\|\hat{\pi}\left(\mathsf{enc}_1(x_1),...,\mathsf{enc}_n(x_n)\right)-\pi(x^n)\right\|\right],$$

受通信和差分隐私约束（其中 $\|\cdot\|$ 可以是 ℓ_1 或 ℓ_2^2）。

3 相关工作

联邦学习与分布式均值估计。 联邦学习 [63, 67, 59] 作为一种去中心化机器学习框架应运而生，通过将客户端的原始数据保留在边缘设备上来保障数据机密性。在联邦学习中，客户端与中央服务器之间的通信很快就会成为瓶颈 [67], ，因此以往的研究主要通过梯度量化[67, 10, 48, 73, 78, 76, 24], 稀疏化 [18, 55, 41]来压缩本地模型更新。为了进一步增强数据安全性，联邦学习通常与差分隐私 [38, 1, 9]结合使用。在这些研究中， [55] 也采用梯度稀疏化（或梯度子采样）来降低问题维度。然而，稀疏化发生在本地梯度聚合之后，因此稀疏化过程中引入的随机性无法用于增强差分隐私保证。因此，与我们的方案相比，这种方法在隐私与通信之间只能实现次优权衡。

请注意，在本工作中，我们研究的是服务器可信的中心化差分隐私设置下的联邦学习（更具体地说，分布式均值估计），这与本地差分隐私模型 [62, 37, 69, 75, 22,32] 以及采用安全聚合的分布式差分隐私模型 [23, 21, 58, 8, 33, 34]不同。

我们均值估计方案的一个关键步骤是通过 Kashin 表示 [66]对本地数据进行预处理。尽管近期文献提出了多种基于量化、稀疏化和抖动的压缩方案，但也有少数研究探索了 Kashin 表示在提升通信效率 [47, 72, 29, 70] 以及实现本地差分隐私 [42] 方面的应用；在联合通信与隐私约束下，它尤其有效，因为它有助于将向量中的信息均匀分散到每个维度。

分布式频率估计与重频项估计。 分布式频率估计（又称直方图估计）是另一项典型任务，已在采用差分隐私的分布式场景下得到广泛研究。以往工作要么关注：1）有或没有通信约束的本地差分隐私模型，例如，[20, 19, 25, 26, 56] （在重频项估计中采用 ℓ_∞ 损失）以及 [57, 79, 75, 6, 5, 32, 46, 71, 45] （采用 ℓ_1 或 ℓ_2 损失）；要么关注 2）不带通信约束的中心化差分隐私模型 [38, 52, 64, 27, 13, 80, 36]。正如 [37, 3, 2, 4, 16], 所指出的，与中心化差分隐私相比，本地差分隐私模型通常会导致更大的估计误差，并显著降低效用。在本工作中，我们研究的是带有明确通信约束的中心化差分隐私。

带洗牌的本地差分隐私。近期一系列研究 [40, 35, 12, 43, 50, 51] 探讨了洗牌差分隐私，表明通过随机洗牌本地（经隐私处理的）消息，可以显著增强中心化差分隐私的保证。在这项工作中，我们表明，同一种洗牌技术也可以在通信开销几乎最优的情况下，实现最优的中心化差分隐私误差。因此，我们可以在通信开销较小的情况下实现同等水平的中心化差分隐私，同时放宽安全性假设：实现最优通信开销（在中心化差分隐私下）只需要一个安全洗牌器（而非完全可信的中央服务器）。

[3]请注意，ℓ_1 误差对应于真实频率向量与估计频率向量之间的全变差距离。 rs.

4 分布式均值估计

在本节中，我们提出一种均值估计方案，在 $(\varepsilon,\ \delta)$-差分隐私下达到最优的 $\tilde{O}_\delta\left(\frac{C^2d}{n^2\varepsilon^2}\right)$ 误差，同时每个客户端仅需通信 $\tilde{O}(n\varepsilon^2)$ 比特。

我们首先考虑一个稍简单的离散设置，其中采用 ℓ_∞ 几何（与第 2 节所述的 ℓ_2 均值估计相对）：假设每个客户端观测到 $x_i \in \{-c,c\}^d$，其中 $c>0$ 为常数；中央服务器旨在估计均值 $\mu(x^n) := \frac{1}{n}\sum_{i=1}^n x_i$，方法是在满足隐私与通信约束的条件下，最小化 ℓ_2^2 误差。我们将在后文论证，上述 ℓ_∞ 问题的解决方案可以通过应用 Kashin 表示用于 ℓ_2 均值估计。

为了解决上述 ℓ_∞ 均值估计问题，首先注意到，每个客户端的本地数据都可以用 d 比特表示，因为 x_i 的每个坐标只能取 $\{c,-c\}$中的值。为了将通信负载降低至 $o(d)$ 比特，每个客户端采用以下子采样策略：对于每个坐标 $j\in[d]$，客户端 i以概率 γ选择向服务器发送 $x_i(j)$。我们假设该子采样步骤使用客户端与服务器共享的种子执行[4],，因此服务器知道每个客户端传输了哪些坐标。于是，在接收到客户端消息后，服务器可以计算每个坐标的均值，并通过添加高斯噪声将其隐私化。我们利用的关键观察是，压缩算法中的随机性可以用于放大隐私，或者等价地，减小隐私化所需的高斯噪声幅度。需要注意的是，这种随机性必须对对手保密，因为该方案的隐私保证依赖于这种随机性。

算法 1 坐标子采样高斯机制（CSGM）

输入：用户数据 $x_1,...,x_n$，采样参数 $\gamma := b/d$，差分隐私参数 (ε,δ)。输出：均值估计量 $\hat{}\mu$。对于用户 $i\in[n]$，对每个坐标 $j\in[d]$，独立同分布地抽取 $Z_{i,j}$，服从伯努利分布 Bern(γ)。如果 $Z_{i,j}=1$，则向服务器发送 $x_i(j)$。结束条件判断。结束坐标循环。结束用户循环。对于每个坐标 $j\in[d]$，服务器计算平均值 $\hat{}\mu_j := \frac{1}{n\gamma}\sum_{i:Z_{ij}=1} x_i(j) + N(0,\sigma^2)$，其中 σ^2 根据定理 4.1 中的式 (1) 计算。结束坐标循环。返回：$\hat{}\mu := (\hat{}\mu_1, \hat{}\mu_2, ..., \hat{}\mu_d)$。

我们在算法 1 中总结了该方案，并在下述定理中陈述其隐私和效用保证。

定理 4.1 (ℓ_∞ 均值估计。)。 设 $x_1,...,x_n\in\{-c,c\}^d$ 且设

$$\sigma^2 = O\left(\frac{c^2\log(1/\delta)}{n^2\gamma^2} + \frac{c^2d(\log(d/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right). \tag{1}$$

那么，对于任意 ε、$\delta>0$，算法 *1* 是(ε,δ)-差分隐私，并在 μ 上产生一个无偏估计量。此外，（平均）每客户端通信成本为 $\gamma\cdot d = b$ 比特，而 $\hat{}\mu$ 的 ℓ_2^2 估计误差至多为

$$\begin{aligned}\mathbb{E}\left[\|\hat{\mu}-\mu\|_2^2\right] &\le \frac{dc^2}{n\gamma} + d\sigma^2 \\ &= O\Big(\frac{d^2c^2}{nb} + \frac{d^3c^2\log(d/\delta)}{n^2b^2} + \frac{c^2d^2(\log(1/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\Big).\end{aligned} \tag{2}$$

[4]在实践中，双方可以提前约定这种随机性，也可以由服务器生成后通信给每个客户端。

注释 4.2 (无偏性)。 请注意，在均值估计中，我们通常希望最终的均值估计量是无偏的，因为随机梯度下降（*SGD*）的标准收敛性分析 *[49]* 要求每一轮优化中对真实梯度的估计无偏。鉴于我们提出的均值估计方案（下一节中的算法 *1* 和算法 *2*）均为无偏的，因此可以将它们与随机梯度下降/联邦平均相结合，并直接应用*[49]*，从而为所得的通信高效差分隐私随机梯度下降（*DP-SGD*）提供收敛保证。

对于第 2 节中提出的 ℓ_2 均值估计任务，我们首先计算局部向量的 Kashin 表示，再进行随机舍入 [61, 74, 42, 32]，以此对其进行预处理。具体而言，若 x_i的 ℓ_2 范数有界于 C，则其相对于紧框架 $K \in \mathbb{R}^{d\times D}$ （其中$D = \Theta(d)$）的 Kashin 表示 $\tilde{x}_i$具有有界的 ℓ_∞ 范数： $\|\tilde{x}_i\|_\infty \le c = O\left(\frac{C}{\sqrt{d}}\right)$，且满足 $x_i = K\cdot\tilde{x}_i$。这使我们能够将 ℓ_2 几何转换为 ℓ_∞ 几何。此外，通过将 $\tilde{x}_i$ 的每个坐标随机舍入为$\{-c, c\}$（例如参见 [32]），我们可以直接应用算法 1，并由此推导出以下 ℓ_2 均值估计的推论：

推论 4.3 (ℓ_2均值估计。) 设 $x_1, ..., x_n \in \mathcal{B}_2(C)$ （即，对于所有 $i \in [n]$， $\|x_i\|_2 \le C$）。那么对于任意 $\varepsilon, \delta > 0$，算法 *1* 结合 *Kashin* 表示和随机舍入，可得到一个(ε, δ)-差分隐私无偏估计量，用于估计 μ，其 ℓ_2^2 估计误差有界为

$$O\left(\underbrace{\frac{dC^2}{nb} + \frac{C^2d^2\log(1/\delta)}{n^2b^2}}_{(\alpha)} + \underbrace{\frac{C^2d(\log(d/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}}_{(\beta)}\right). \tag{3}$$

推论 4.3 中估计误差的第一项（α）是由压缩导致的误差，第二项（β）是由隐私化导致的误差（在 (ε, δ)-差分隐私下，该误差在相差一个额外的 $\log(d/\delta)$ 因子的范围内达到阶最优，详见第 4.2 节）。特别地，忽略多对数项并假设 $\varepsilon = O(1)$，隐私化误差（β）可简化为 $\tilde{O}\left(\frac{dC^2}{n^2\varepsilon^2}\right)$。当 $b = \tilde{\Omega}_\delta\left(\max\left(n\varepsilon^2, \sqrt{d}\varepsilon\right)\right)$ 时，该误差主导总均值估计误差 ℓ_2^2，也就是说，在此情形下，总 ℓ_2^2 误差的阶与集中式差分隐私的最优误差（β）相同。这意味着，在 (ε, δ)-差分隐私下，要达到阶最优的 ℓ_2^2 误差，每个客户端所需的比特数不超过 $b = \tilde{\Omega}_\delta\left(\max\left(n\varepsilon^2, \sqrt{d}\varepsilon\right)\right)$。

在下一节中，我们将介绍对算法 1 的一种修改，以去除通信开销中的 $\Omega\left(\sqrt{d}\varepsilon\right)$项。

4.1 无维度通信成本

为了消除上一节中通信开销 $b = \tilde{\Omega}_\delta\left(\max\left(n\varepsilon^2, \sqrt{d}\varepsilon\right)\right)$对维度 d 的依赖，我们需要提升方案在小样本 情形$n\varepsilon^2 = o(\sqrt{d}\varepsilon)$下的性能。等价地，当 $n\varepsilon = o(\sqrt{d})$时，我们希望仅使用每个客户端 $b = \tilde{\Omega}_\delta\left(n\varepsilon^2\right)$ 比特，就能达到集中式差分隐私性能。假设 $\varepsilon \approx 1$，注意到这意味着系统的总通信带宽为 $nb = o(d)$，也就是说，服务器最多只能接收关于$nb = n^2\varepsilon^2 = o(d)$个坐标的信息。我们将证明，在这一情形下，通过预先将服务器的关注范围限制在坐标的一个子集上，可以提升方案的性能。

我们对算法 1 作如下修改：在执行算法 1 之前，服务器随机选择 $d' \approx O\left(\min(d, n^2\varepsilon^2)\right)$ 个坐标，并且只要求客户端在这些坐标上运行算法 1。我们在算法 2 中给出修改后的方案，并在定理 4.4 中总结其性能。

S同样，我们可以通过 Kashin 表示获得如下均值估计 s:

定理 4.4 (ℓ_2均值估计。)。 令 $x_1, ..., x_n \in \mathcal{B}_2(C)$ *(*即，对所有 $i \in [n]$， $\|x_i\|_2 \le C$*)*， $d' = \min\left(d, nb, \frac{n^2\varepsilon^2}{1/\delta + \varepsilon(\log(\cdot))\log(d/\delta)}\right)$，并且

$$\sigma^2 = O\left(\frac{C^2\log(1/\delta)}{d'n^2\gamma^2} + \frac{C^2d'(\log(1/\delta)+\varepsilon)\log(d'/\delta)}{dn^2\varepsilon^2}\right). \tag{4}$$

算法 2 带坐标预选的 CSGM

输入：用户数据 $x_1, ..., x_n$，坐标选择 $d' \le d$，采样参数 $\gamma := b/d'$，差分隐私参数 (ε, δ)。输出：均值估计量 $\hat{\mu}$。随机选择 d' 个坐标 $\mathcal{J} := \{j_1, ..., j_{d'}\} \subset [d]$。对于用户 $i \in [n]$，通过将其限制在 $\mathcal{J}$ 来设 $x_i(\mathcal{J}) := (x_i(j_1), ..., x_i(j_{|\mathcal{J}|}))$ 上进行预处理 x_i。结束循环。对 $x_i(\mathcal{J})$ $i \in [n]$ 应用 CSGM（算法 1）：$\hat{\mu}_{\mathcal{J}} \leftarrow \text{CSGM}(x_i(\mathcal{J})\ i \in [n])$。对于 $j \in [d]$，如果 $j \in \mathcal{J}$，则 $\hat{\mu}_j = \hat{\mu}_{\mathcal{J}}(j)$；否则 $\hat{\mu}_j = 0$。结束条件。结束循环。返回：$\hat{\mu} := \left(\frac{d}{d'}\hat{\mu}_1, \frac{d}{d'}\hat{\mu}_2, ..., \frac{d}{d'}\hat{\mu}_d\right)$。

那么，对于任意 ε、$\delta > 0$，算法 2 满足(ε, δ)-差分隐私。此外，（平均）每客户端通信成本为 $\gamma d = b$ 比特，且均值估计误差至多为

$$O\left(\max\left(\frac{C^2 d \log(d/\delta)}{nb}, \frac{C^2 d \log(d/\delta)(\log(1/\delta) + \varepsilon)}{n^2\varepsilon^2}\right)\right). \tag{5}$$

推论 4.5。只要 $b = \Omega\left(\frac{n\varepsilon^2}{\log(1/\delta)+\varepsilon}\right)$，均值估计的误差就是

$$O\left(\frac{C^2 d \log(d/\delta)(\log(1/\delta) + \varepsilon)}{n^2\varepsilon^2}\right).$$

如推论 4.5 所示，当 $\varepsilon = O(1)$ 时，每个客户端使用 $b = \tilde{\Omega}\left(n\varepsilon^2\right)$ 比特就足以达到阶最优的 $\tilde{O}_\delta\left(\frac{C^2 d}{n^2\varepsilon^2}\right)$ 误差（即使在小样本情形 $n \le \sqrt{d}$ 下也如此），也就是说，该方案的通信开销与维度 d 无关。

4.2 下界

在本节中，我们论证定理 4.4 中的估计误差在一个 $\log(d/\delta)$ 因子范围内是最优的。具体而言，[31] 的定理 5.3 表明，任何 b 比特的无偏压缩方案，在 ℓ_2 均值估计问题中都会产生 $\Omega\left(\frac{C^2 d}{nb}\right)$ 误差（即使不要求隐私）。这与式 (5) 中的第一项相差一个对数因子。

另一方面，集中式高斯机制（在中心化 (ε, δ)-差分隐私下）可达到 $O\left(\frac{C^2 d \log(1/\delta)}{n^2\varepsilon^2}\right)$ 均方误差 [15]（在大多数参数范围内，这是阶最优的；参见 [28] 的定理 3.1 中的下界，或 [30] 的命题 23）。因此，我们可以得出结论：若要达到与高斯机制相同的误差，服务器接收的总通信量至少要为 $\Omega(n^2\varepsilon^2)$ 比特。因此，每客户端的平均通信开销至少要为 $\Omega(n\varepsilon^2)$ 比特。由此可见，算法 2 是最优的（相差一个对数因子）。

F为完整起见，我们在以下定理中陈述通信下界：

定理 4.6（中心化差分隐私下均值估计的通信下界）。设 $x_1, ..., x_n \in \mathcal{B}_2(C)$。令 $Y_1, ..., Y_n$ 为由（可能交互式的）压缩器生成的任意 b 位本地报告，并且在以下意义下无偏：

满足

$$\mathbb{E}\left[\sum_i Y_i\right] = \sum_i x_i.$$

那么，如果

$$\mathbb{E}\left[\left\|\frac{1}{n}\sum_i Y_i - \frac{1}{n}\sum_i x_i\right\|_2^2\right] \le O\left(\frac{C^2 d\log(1/\delta)}{n^2\varepsilon^2}\right),$$

则有

$$b = \Omega\left(\frac{n\varepsilon^2}{\log(1/\delta)}\right).$$

最后，我们指出，上界与下界之间的对数级差距，可能是由于我们在证明中采用了特定的组合定理（[39]的定理 III.3）所致。该定理更易于处理，但可能略弱。不过，在实验中，我们使用 Rényi 差分隐私计算并考虑了所有隐私预算，因此相较于理论分析，可以得到更好的常数。

5 分布式频率估计

本节讨论联邦分析中的频率估计问题。回顾一下，对于频率估计任务，每个客户端的私有数据 $x_i \in \{0,1\}^d$ 满足 $\|x_i\|_0 = 1$，目标是通过最小化 ℓ_2（或 ℓ_1，ℓ_∞）误差 $\mathbb{E}\left[\|\pi - \hat{\pi}(Y^n)\|_2^2\right]$，在满足通信和（$\varepsilon$，$\delta$）差分隐私约束的条件下估计 $\pi := \frac{1}{n}\sum_i x_i$。上下文明确时，我们有时会滥用记号，用 x_i 表示项目的索引，即 $x_i \in [d]$。

为了充分利用问题的 ℓ_0 结构，一种标准方法是应用哈达玛变换，将 ℓ_0 几何结构转换为 ℓ_∞ 几何结构，然后利用哈达玛矩阵的递归结构，高效地压缩本地消息。

具体而言，对于给定的 b，其约束为 2^{b-1}，我们将每个本地项 x_i 划分为 2^{b-1} 个块，注意，由于 x_i 是独热的，因此 $x_i^{(j)}$ 中只有一个块非零。然后，客户端 i 对每个块执行以下哈达玛变换：$y_i^{(\ell)} = H_B \cdot x_i^{(\ell)}$，其中 H_B 的递归定义如下：

$$H_{2^n} = \frac{1}{\sqrt{2}}\begin{bmatrix} H_{2^{n-1}}, & H_{2^{n-1}} \\ H_{2^{n-1}}, & -H_{2^{n-1}} \end{bmatrix}, \text{ and } H_0 = [1].$$

随后，每个客户端通过服务器也知晓的共享随机性生成一个采样向量 $Z_{ij} \overset{\text{独立同分布地}}{\sim}$ 伯努利分布，并将 $(y_i^{(1)}(j)$ ……，$y_i^{(2^{b-1})}(j))$ 作为其本地报告提交。由于 $(y_i^{(1)}(j)$ ……，$y_i^{(2^{b-1})}(j))$ 仅包含一个非零条目，且该条目可以为 $\frac{1}{\sqrt{B}}$ 或 $-\frac{1}{\sqrt{B}}$，因此本地报告可以用 b 比特表示（其中 $b-1$ 比特用于表示非零条目的位置，1 比特用于表示其符号）。

服务器可以通过将本地报告相加（进行适当的归一化），并执行逆哈达玛变换，从中计算出一个无偏估计量。此外，在适当注入高斯噪声后，该频率估计量满足 $(\varepsilon,\ \delta)$-差分隐私。

这一思想已在采用本地差分隐私的既有研究中得到应用 [19, 6, 3, 32],，但为了在中心-差分隐私下获得阶数最优的权衡，需要将哈达玛变换与随机子采样步骤相结合，并在分析中纳入由随机压缩带来的隐私放大。在算法 3 中，我们总结了所得方案。该方案建立在 [32], 的递归哈达玛响应（RHR）机制之上，该机制最初是为本地 差分隐私下的通信高效频率估计而设计的。

在以下定理中，我们控制算法 3 的 ℓ_∞ 误差。

定理 5.1。 设 $\hat{\pi}(x^n)$ 为算法 *3* 的输出。那么，对于所有 $j \in [d]$，均有：

$$\mathbb{E}\left[|\pi(j) - \hat{\pi}(j)|\right] \le \sqrt{\frac{\sum_i \mathbb{1}_{\{x_i \in [B\cdot(j-1):B\cdot j-1]\}}}{n^2} + \frac{\sigma^2}{B}}, \tag{6}$$

算法 3 子采样递归哈达玛响应

输入： 用户数据 x_1，……，$x_n \in \{0,1\}^d$（其中 d 是 2 的幂），差分隐私参数（ε，δ），通信预算 b。

输出： 频率估计 $\hat{}\pi$设定 $B := d/2^{b-1}$，并将每个独热向量 x_i 划分为 2^{b-1} 个数据块：$x_i^{(1)}$，……，$x^{(2^b-1)}{}_i \in \{0,1\}^B$。**对于**用户 $i \in [n]$ **执行**计算每个数据块的哈达玛变换：$y_i^{(\ell)} = H_B \cdot x_i^{(\ell)}$.
对于坐标 $j \in [B]$ **执行**抽取 $Z_{i,\ j}$ 独立同分布∼ 伯努利分布 $\left(\frac{1}{B}\right)$**如果**$Z_{i,\ j} = 1$ **那么**发送 $(y_i^{(1)}(j)$，……，$y_i^{(2^{b-1})}(j))$ 至服务器。**结束条件判断，结束循环，结束循环**服务器计算平均值：$\forall \ell \in [2^{b-1}]$, $j \in [B]$,

$$\hat{y}^{(\ell)}(j) := \frac{B}{n} \sum_{i:Z_{ij}=1} y_i^{(\ell)}(j) + N(0,\sigma^2),$$

其中，σ^2 根据定理 5.2 计算。
服务器对 $\hat{}\pi^{(\ell)} = H_B \cdot \hat{}y^{(\ell)}$，执行逆哈达玛变换，以处理 $\ell = 1$，……，B。
返回： $\hat{}\pi = \left(\left(\hat{}\pi^{(1)}\right)$，……，$\left(\hat{}\pi^{(2^b-1)}\right)\right)$。

且 ℓ_2^2 与 ℓ_1 误差有界，满足

$$\mathbb{E}\left[\|\pi - \hat{\pi}\|_2^2\right] \le \frac{B}{n} + \frac{d\sigma^2}{B}, \ and \tag{7}$$

$$\mathbb{E}\left[\|\pi - \hat{\pi}\|_1\right] \le \sqrt{\frac{dB}{n} + \frac{d^2\sigma^2}{B}}. \tag{8}$$

定理 5.2。对于任意 $\varepsilon, \delta > 0$，若满足以下条件，则算法 *3* 是(ε, δ)-差分隐私：

$$\sigma^2 \ge O\left(\frac{B^2 \log(B/\delta)}{n^2} + \frac{B(\log(1/\delta)+\varepsilon)\log(B/\delta)}{n^2\varepsilon^2}\right).$$

结合定理 5.1 和定理 5.2，可得算法 3 实现了 $(\varepsilon,\ \delta)$-差分隐私，其 ℓ_2^2误差为

$$\begin{aligned} &O\left(\frac{B}{n} + \frac{dB\log(B/\delta)}{n^2} + \frac{d(\log(1/\delta)+\varepsilon)\log(B/\delta)}{n^2\varepsilon^2}\right) \\ &= O\left(\frac{d}{n2^b} + \frac{d^2\log(d/\delta)}{n^2 2^b} + \frac{d(\log(1/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right). \end{aligned}$$

˜注意，当 $n = \Omega(d)$ 时，误差可简化为

$$O\left(\frac{d}{n2^b} + \frac{d(\log(1/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right),$$

这与在比特数约束 [54, 3, 2]和 (ε,δ)-差分隐私约束 [15, 7]下的阶数最优估计误差相匹配（相差一个 $\log d$ 因子）。

6 通过洗牌实现最优权衡

在第4节和第5节中，我们看到，只要服务器是可信的，通信开销就可以降至（均值估计为 $\tilde{O}\left(n\varepsilon^2\right)$，频率估计为 $\tilde{O}\left(\log\left(\lceil n\varepsilon^2\rceil\right)\right)$），同时仍能达到阶数意义下的最优误差。另一方面，当服务器不可信时，[33, 31] 表明，借助安全聚合可以在 (ε,δ)-差分隐私下达到最优误差。不过，这些方案的通信开销在均值估计中为每个客户端 $\tilde{O}\left(n^2\varepsilon^2\right)$ 比特，在频率估计中为每个客户端 $\tilde{O}(n\varepsilon)$ 比特。这相当于均值估计的通信开销增加 n 倍，而频率估计的通信开销则呈指数级增长。本节探讨，当服务器并非完全可信时，能否实现前几节所述的最优通信-准确性-隐私权衡。

本节将说明，如果存在一个安全 洗牌器，能够随机排列客户端本地隐私化后的消息并将其发布给服务器，那么我们就能以 $\tilde{O}\left(n\varepsilon^2\right)$ 比特的通信量，实现均值估计中近乎最优（相差一个 $\log d$ 因子）的中心化差分隐私误差。具体而言，我们基于以下近期结果 [40, 43]，提出一种将本地差分隐私机制与通过洗牌实现的隐私放大相结合的均值估计方案：

引理 6.1 ([43])。 设对于每个 $i\in[n]$， $\mathcal{M}_i$ 都是一个独立的$(\varepsilon_0,0)$-本地差分隐私机制，满足 $\varepsilon_0\le 1$，且 π 是 $[n]$的一个随机排列。那么，对于任意满足 $\varepsilon_0\le\log\left(\frac{n}{16\log(2/\delta)}\right)$ 的 $\delta\in[0,1]$，该机制

$$\mathcal{S}:(x_1,\ldots,x_n)\mapsto\left(\mathcal{M}_1\left(x_{\pi(1)}\right),\ldots,\mathcal{M}_n\left(x_{\pi(n)}\right)\right)$$

是(ε,δ)-差分隐私，对于某个满足 $\varepsilon=O\left(\varepsilon_0\frac{\sqrt{\log(1/\delta)}}{\sqrt{n}}\right)$ 的 ε。

隐私分析。 利用上述放大引理，我们只需设计满足 ε_0-本地差分隐私的本地随机化器 $\mathcal{M}_i$。注意，只有当 $\varepsilon_0=O(1)$ 时，上述引理才是紧的，因此限制了（放大后的）中心差分隐私 $\varepsilon=O(1/\sqrt{n})$ 必须非常小。为适应更大的 ε，用户可以在不同的洗牌轮次中，分别向服务器发送消息的不同部分。等价地，我们重复执行洗牌后的本地差分隐私机制 $T=O\left(\lceil n\varepsilon^2\rceil\right)$ 轮，同时确保客户端在每一轮中都向服务器传递关于其样本的独立信息。具体而言，在每一轮中，每个客户端使用每轮局部隐私预算 $\varepsilon_0=O(1)$ 应用本地随机化器 $\mathcal{M}_i$，并向服务器发送一条独立消息。这样，每轮都会得到（放大后的）中心差分隐私 $O(1/\sqrt{n})$，根据组合定理 [57]，经过 $T=O\left(\lceil n\varepsilon^2\rceil\right)$ 轮组合后，整体方案满足 ε-差分隐私。我们在附录 E 的算法 4 中详细说明该算法。

备注 6.2。 尽管我们的分析主要聚焦于(ε,δ)-差分隐私，但利用近期的放大结果 *[44]*，也可以获得 ***Rényi*** 差分隐私保证（这可能有助于实际的隐私核算）。

通信成本。 上述 T 轮方案的通信成本可按如下方式计算。如 [32]，所示， ε_0-本地差分隐私均值估计的最优通信成本为 $O(\lceil\varepsilon_0\rceil)$ 比特。此外， [32] 中提出的（私有随机币）SQKR 方案使用 $O\left(\lceil\varepsilon_0\rceil\log d\right)$ 比特进行通信（该方案的正式性能保证见引理 6.3），其中压缩通过对坐标进行子采样实现，隐私化则采用随机响应。因此，由于每轮$\varepsilon_0=O(1)$，每客户端的总通信成本为 $O\left(n\varepsilon^2\log d\right)$，在 $\log d$ 因子范围内达到第4节中的最优通信下界。

引理 6.3 (SQKR [32])。 对于所有 $\varepsilon_0>0$、$b_0>0$，存在一个$(\varepsilon_0,0)$-本地差分隐私机制 $x_i\mapsto\hat{}\mu$，使用$b_0\log(d)$ 比特，使得$\hat{}\mu$ 是无偏的，并满足

$$\mathbb{E}\left[\left\|\mu\left(x^n\right)-\hat{\mu}\left(x^n\right)\right\|_2^2\right]=O\left(\frac{c^2d}{n\min\left(\varepsilon_0^2,\varepsilon_0,b_0\right)}\right).$$

最后，我们在以下定理中总结整体方案（算法 4）的性能保证。

定理 6.4 （ℓ_2均值估计）。 设 $x_1, ..., x_n \in \mathcal{B}_2(C)$ （即，对于所有 $i \in [n]$， $\|x_i\|_2 \le C$）。对于所有 $\varepsilon > 0, b > 0, n > 30$ 和 $\delta \in (\delta_{\min}, 1]$，其中 $\delta_{\min} = O\left(\frac{be^{-n}}{d \log()}\right)$，算法 *4* 结合 *Kashin* 表示和随机舍入后满足 (ε, δ)-差分隐私，通信量不超过 b 比特，并且达到

$$\mathbb{E}\left[\left\|\mu\left(x^n\right) - \hat{\mu}\left(x^n\right)\right\|_2^2\right] = O\left(C^2 d \max\left(\frac{\log(d)}{nb}, \frac{\log(b/\delta)(\log(1/\delta)+\varepsilon)}{n^2\varepsilon^2}\right)\right).$$

注 6.5. 与先前的方案算法 *1–3* 不同，洗牌 *SQKR* 对 δ 有一定要求，即 $\delta \in [\delta_{min}, 1]$，这是由我们使用的特定洗牌引理导致的。不过在实践中，由于对 n 的指数依赖， $\delta_{\min}$ 较小。当 $b = \Omega_\delta\left(n \log(d) \min\left(\varepsilon^2, \varepsilon\right)\right)$ 时，$O\left(n^2 \frac{C^2 d}{\min(\varepsilon^2, \varepsilon)}\right)$ 可达到阶数意义下的最优误差（相差对数因子）。

注 6.6. 我们注意到，先前已有研究探讨了基于洗牌的私有均值估计的类似思路，例如 *[53]*。然而，这些论文未在多轮中使用上述隐私预算拆分技巧，因此只有当 ε 非常小时，其结果才是最优的。上述方案可视为一种多消息洗牌方案 *[35, 51],* ，特别是可以看作将标量均值估计方案 *[35]* 推广到 d 维均值估计的推广方案。

7 实验

在本节中，我们通过实证评估第4节提出的均值估计方案（CSGM），考察其隐私-准确率-通信权衡，并将其与其他差分隐私机制（包括第6节介绍的基于洗牌的机制）进行比较。

设置。 对于给定的维度 d 和样本数量 n，我们按如下方式生成本地向量 $X_i \in \mathbb{R}^d$： 令 $X_i(j) \overset{\text{独立同分布}}{\sim} \frac{1}{\sqrt{d}}(2 \cdot$ 伯努利分布$(0.8) - 1)$，其中伯努利分布(0.8)是一个偏置为 $p = 0.8$ 的伯努利随机变量。这确保了 $\|X_i\|_\infty \le 1/\sqrt{d}$ 和 $\|X_i\|_2 \le 1$，此外，经验均值 $\mu(X^n) := \frac{1}{n}\sum_i X_i$ 不会收敛到 0。请注意，由于我们的目标是构造一个无偏估计量，我们没有将最终估计量投影回 ℓ_∞ 或 ℓ_2 空间，因为投影步骤可能引入偏差。因此， ℓ_2 估计误差可能大于 1。我们使用 R´ényi 差分隐私 [68] 和 [81] 中的子抽样隐私放大引理来核算隐私预算，并通过 [30]将 R´ényi 差分隐私转换为 (ε, δ)-差分隐私。

CSGM 的隐私-准确率-通信权衡。 在第一组实验（图 1）中，我们使用不同的采样率 γ 应用算法 1，从而得到不同的通信预算（$b = \gamma d$）。请注意，当 $\gamma = 1$ 时，该方案退化为不使用压缩的中心化高斯机制。在图 1 中可以看到，在通信预算固定时，CSGM 在高隐私区间（ ε 较小时）近似于中心化（未压缩）高斯机制，而当 ε 超过某个值时，便开始偏离该机制。此外， ε 的这一临界值仅取决于样本量 n 和通信预算 b，而与维度 d 无关，这与我们的理论预测一致：回想一下，压缩误差占总误差的主导地位，因此，当 $b = o$（$n\varepsilon^2$）时，性能便开始偏离（未压缩）高斯机制；这一条件与 d 无关。例如，当 $b = 50$ 比特时，对于 $d = 500$ 和 $d = 5000$，高斯机制均在 $\varepsilon \ge 0.5$ 时开始优于 CSGM。因此，对于 $\varepsilon \approx 0.5$ ，当 $d = 500$ 时，CSGM 能够实现 10 倍压缩；而当 $d = 5000$ 时，则能实现 100 倍压缩，且不影响均方误差。

与本地差分隐私和洗牌差分隐私的比较。 接下来，我们比较 CSGM 与本地差分隐私和洗牌差分隐私在$d = 10^3$ 和 $n = 500$下的表现。对于本地差分隐私，我们考虑第 6 节中介绍的私有硬币 SQKR 方案；当 $\varepsilon \le 1$ 时，该方案使用 $\lceil \log d \rceil = 10$ 比特。我们还考虑 DJW [37]，已知它在 $\varepsilon = O$时是阶最优的（但通信效率不高）。对于洗牌差分隐私，我们应用 [43]中的放大引理，求得相应的本地 ε_0 （更多细节见第 6 节），并将 SQKR 和 DJW 都模拟为本地随机化器。我们注意到，本实验中考虑的所有洗牌差分隐私机制都是单轮的（而非第 6 节中的多轮方案），这在高隐私区间（即 ε 较小时）是最优的。

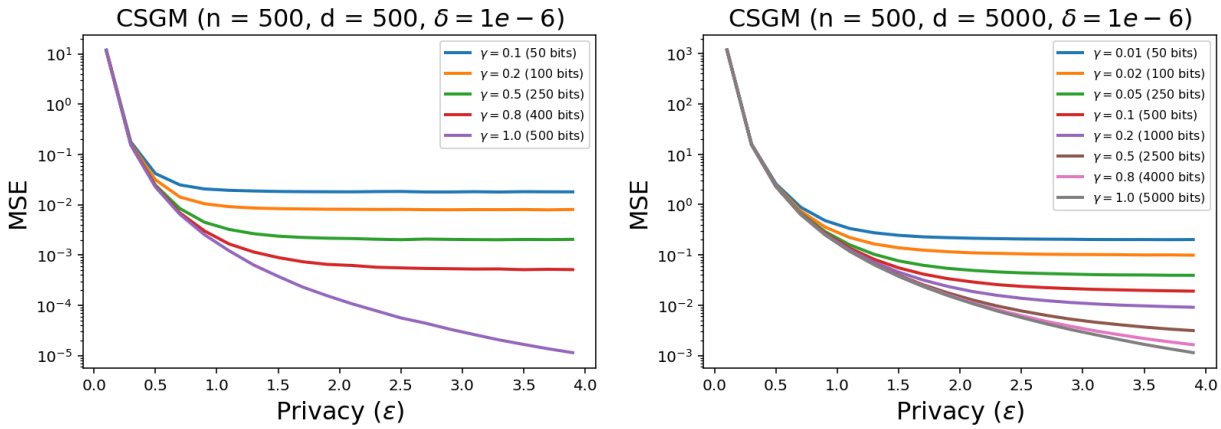

图 1：低维（左）和高维（右）情况下 CSGM（算法 1）的均方误差。

所有机制的均方误差均见图2。我们的结果表明，在通信预算固定时（例如 10 比特），CSGM 的实际表现优于洗牌差分隐私机制，包括洗牌 SQKR 和 DJW。此外，随着 ε 增大，洗牌带来的放大增益会迅速减弱。事实上，当 $\varepsilon \geq 0.8$时，我们观察到与纯本地差分隐私相比没有放大增益。

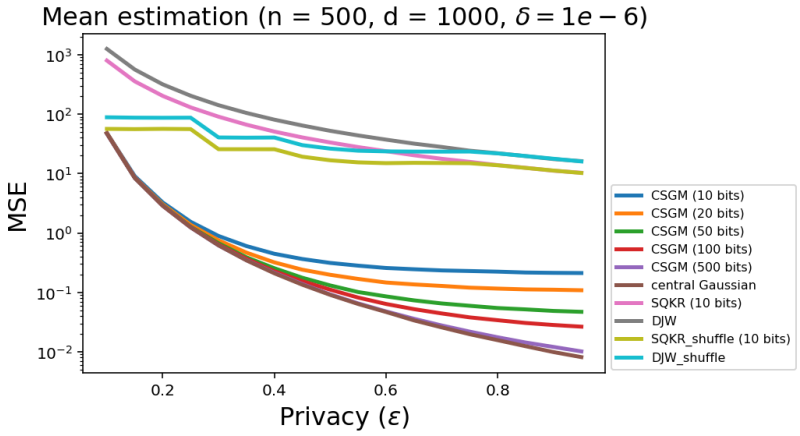

图2：与本地差分隐私和洗牌差分隐私的比较。

参考文献

[1] M. Abadi、A. Chu、I. Goodfellow、H. B. McMahan、I. Mironov、K. Talwar 和 L. Zhang。《差分隐私深度学习》。载于*2016*年*ACM SIGSAC*计算机与通信安全大会论文集，第 308–318 页，2016年。

[2] J. Acharya、C. L. Canonne 和 H. Tyagi。《信息约束下的推断 II：通信约束与共享随机性》。*arXiv* 预印本 *arXiv:1905.08302*，2019年。

[3] J. Acharya、C. L. Canonne 和 H. Tyagi。《信息约束下的推断：基于卡方收缩的下界》。载于学习理论会议，第 3–17 页。PMLR，2019年。

[4] J. Acharya、C. L. Canonne 和 H. Tyagi。在信息约束下交互式高维估计的一般下界。*arXiv*预印本 *arXiv:2010.06562*，2020年。

[5] J. Acharya 和 Z. Sun。本地差分隐私分布估计与重频项问题中的通信复杂度
重频项。在国际机器学习会议，第51–60页，2019年。[6] J. Acharya、Z. Sun 和 H. Zhang。Hadamard响应机制：以保护隐私、高效且低通信开销的方式估计分布。发表于第*22*届国际人工智能与统计会议，第1120–1129页，2019年。[7] J. Acharya、Z. Sun 和 H. Zhang。差分隐私Assouad方法、Fano方法和 Le Cam方法。发表于算法学习理论，第48–78页。PMLR，2021年。[8] N. Agarwal、P. Kairouz 和 Z. Liu。用于差分隐私联邦学习的 Skellam 机制。神经信息处理系统进展，34：5052–5064，2021年。[9] N. Agarwal、A. T. Suresh、F. X. X. Yu、S. Kumar 和 B. McMahan。CPSGD：通信高效且保护差分隐私的分布式随机梯度下降。发表于神经信息处理系统进展，第7564–7575页，2018年。[10] D. Alistarh、D. Grubic、J. Li、R. Tomioka 和 M. Vojnovic。QSGD：通过梯度量化和编码实现通信高效的随机梯度下降。发表于第*30*届神经信息处理系统大会，第1709–1720页，2017年。[11] J. Allen、B. Ding、J. Kulkarni、H. Nori、O. Ohrimenko 和 S. Yekhanin。面向可信处理器上差分隐私数据分析的算法框架。神经信息处理系统进展，32，2019年。[12] V. Balcer 和 A. Cheu。通过直方图区分本地差分隐私与洗牌差分隐私。*arXiv*预印本 *arXiv:1911.06879*，2019年。[13] V. Balcer 和 S. Vadhan。有限计算机上的差分隐私。*arXiv*预印本 *arXiv:1709.05396*，2017年。[14] B. Balle、G. Barthe 和 M. Gaboardi。通过子采样实现的隐私放大：基于耦合与散度的紧确分析。神经信息处理系统进展，31，2018年。[15] B. Balle 和 Y.-X. Wang。改进差分隐私的高斯机制：解析校准与最优去噪。发表于国际机器学习会议，第394–403页。PMLR，2018年。[16] L. P. Barnes、W.-N. Chen 和 A. Ozgur。本地差分隐私下的 Fisher 信息。*arXiv*预印本 *arXiv:2005.10783*，2020年。[17] L. P. Barnes、Y. Han 和 A. Ozgur。通过 Fisher 信息，在通信约束下学习分布的下界，2019年。[18] L. P. Barnes、H. A. Inan、B. Isik 和 A. Ozgur。rtop-k：一种分布式随机梯度下降的统计估计方法，2020年。[19] R. Bassily、K. Nissim、U. Stemmer 和 A. Thakurta。实用的本地隐私重频项协议。发表于第*31*届神经信息处理系统国际会议论文集，NIPS'17，第2285–2293页，美国纽约州雷德胡克，2017年。Curran Associates Inc。[20] R. Bassily 和 A. Smith。用于紧凑直方图的本地隐私高效协议。发表于第*47*届*ACM*计算理论年度研讨会论文集，STOC '15，第127–135页，美国纽约，2015年。计算机协会。[21] J. H. Bell、K. A. Bonawitz、A. Gasc´on、T. Lepoint 和 M. Raykova。具有（多项式）对数级开销的安全单服务器聚合。发表于*2020*年*ACM SIGSAC*计算机与通信安全会议论文集，第1253–1269页，2020年。

[22] A. Bhowmick、J. Duchi、J. Freudiger、G. Kapoor 和 R. Rogers。防范重构及其在隐私联邦学习中的应用。*arXiv*预印本 *arXiv:1812.00984*，2018年。[23] K. Bonawitz、V. Ivanov、B. Kreuter、A. Marcedone、H. B. McMahan、S. Patel、D. Ramage、A. Segal 和 K. Seth。面向用户持有数据的联邦学习实用安全聚合。*arXiv*预印本 *arXiv:1611.04482*，2016年。[24] M. Braverman、A. Garg、T. Ma、H. L. Nguyen 和 D. P. Woodruff。通过分布式数据处理不等式，推导统计估计问题的通信下界。发表于第*48*届*ACM*计算理论年度研讨会论文集，第1011–1020页，2016年。[25] M. Bun、J. Nelson 和 U. Stemmer。重频项与本地隐私的结构。发表于第*37*届*ACM SIGMOD-SIGACT-SIGAI*数据库系统原理研讨会论文集，SIGMOD-/PODS '18，第435–447页，美国纽约，2018年。计算机协会。[26] M. Bun、J. Nelson 和 U. Stemmer。重频项与本地隐私的结构。*ACM*算法汇刊（*TALG*），15(4)：1–40，2019年。[27] M. Bun 和 T. Steinke。集中差分隐私：简化、扩展与下界。发表于密码学理论会议，第635–658页。施普林格，2016年。[28] T. T. Cai、Y. Wang 和 L. Zhang。隐私成本：差分隐私下参数估计的最优收敛速率。统计年鉴，49(5)：2825–2850，2021年。[29] S. Caldas、J. Koneˇcny、H. B. McMahan 和 A. Talwalkar。通过降低客户端资源需求，扩大联邦学习的应用范围。*arXiv*预印本 *arXiv:1812.07210*，2018年。[30] C. L. Canonne、G. Kamath 和 T. Steinke。用于差分隐私的离散高斯分布。*arXiv*预印本 *arXiv:2004.00010*，2020年。[31] W.-N. Chen、C. A. C. Choo、P. Kairouz 和 A. T. Suresh。差分隐私联邦学习中安全聚合的根本代价。发表于国际机器学习会议，第3056–3089页。PMLR，2022年。[32] W.-N. Chen、P. Kairouz 和 A. Ozgur。打破通信-隐私-准确率三难困境。神经信息处理系统进展，33，2020年。.[33] W.-N. Chen、A. Ozg¨ur、G. Cormode 和 A. Baharadwaj。联邦频率估计中的安全与隐私通信开销。投稿中，2022年。[34] W.-N. Chen、A. Ozgur 和 P. Kairouz。用于安全聚合下无偏联邦学习的泊松二项机制。发表于国际机器学习会议，第3490–3506页。PMLR，2022年。[35] A. Cheu、A. Smith、J. Ullman、D. Zeber 和 M. Zhilyaev。通过洗牌实现分布式差分隐私。发表于密码技术理论与应用年度国际会议，第375–403页。施普林格，2019年。[36] G. Cormode 和 A. Bharadwaj。抽样阈值差分隐私：直方图及其应用。发表于人工智能与统计国际会议，第1420–1431页。PMLR，2022年。[37] J. C. Duchi、M. I. Jordan 和 M. J. Wainwright。本地隐私与统计极小极大速率。发表于*2013*年*IEEE*第*54*届计算机科学基础年度研讨会，第429–438页。IEEE，2013年。[38] C. Dwork、F. McSherry、K. Nissim 和 A. S mith。为隐私数据分析校准噪声以匹配敏感度。发表于密码学理论会议，第265–284页。施普林格，2006年。[39] C. Dwork、G. N. Rothblum 和 S. Vadhan。提升与差分隐私。发表于*2010*年*IEEE*第*51*届计算机科学基础年度研讨会，第51–60页。IEEE，2010年。

[40] ´U. Erlingsson、V. Feldman、I. Mironov、A. Raghunathan、K. Talwar 和 A. Thakurta。通过洗牌实现隐私放大：借助匿名化从局部差分隐私迈向中心化差分隐私。载于第三十届 *ACM-SIAM* 离散算法年度研讨会论文集，第 2468–2479 页。SIAM，2019年。[41] F. Farokhi。梯度稀疏化可提升差分隐私凸机器学习的性能。载于*2021*年第*60*届 *IEEE* 决策与控制会议，第 1695–1700 页。IEEE，2021年。[42] V. Feldman、C. Guzman 和 S. Vempala。用于均值向量估计和随机凸优化的统计查询算法。载于第二十八届 *ACM-SIAM* 离散算法年度研讨会论文集，第 1265–1277 页。SIAM，2017年。[43] V. Feldman、A. McMillan 和 K. Talwar。隐藏在克隆者之中：对洗牌隐私放大的简明且近乎最优的分析。载于*2021*年 *IEEE* 第*62*届计算机科学基础年度研讨会，第 954–964 页。IEEE，2022年。[44] V. Feldman、A. McMillan 和 K. Talwar。针对 Rényi 差分隐私和近似差分隐私的更强洗牌隐私放大。载于*2023*年 *ACM-SIAM* 离散算法年度研讨会论文集（*SODA*），第 4966–4981 页。SIAM，2023年。[45] V. Feldman、J. Nelson、H. Nguyen 和 K. Talwar。基于射影几何的隐私频率估计。载于国际机器学习会议，第 6418–6433 页。PMLR，2022年。[46] V. Feldman 和 K. Talwar。高效隐私本地随机化器的无损压缩。*arXiv* 预印本 *arXiv:2102.12099*，2021年。[47] J.-J. Fuchs。扩展表示。载于*2011*年第*45*届阿西洛马信号、系统与计算机会议记录（*ASILOMAR*），第 814–817 页。IEEE，2011年。[48] V. Gandikota、D. Kane、R. K. Maity 和 A. Mazumdar。vqsgd：向量量化随机梯度下降，2019年。[49] S. Ghadimi 和 G. Lan。非凸随机规划的随机一阶与零阶方法。*SIAM* 优化期刊，23(4):2341–2368，2013年。[50] B. Ghazi、N. Golowich、R. Kumar、R. Pagh 和 A. Velingker。多条匿名消息的威力。*arXiv* 预印本 *arXiv:1908.11358*，2019年。[51] B. Ghazi、R. Kumar、P. Manurangsi 和 R. Pagh。通过匿名消息实现隐私计数：以极低通信开销实现近乎最优的准确度。载于国际机器学习会议，第 3505–3514 页。PMLR，2020年。[52] A. Ghosh、T. Roughgarden 和 M. Sundararajan。普遍实现效用最大化的隐私机制。*SIAM* 计算期刊，41(6):1673–1693，2012年。[53] A. Girgis、D. Data、S. Diggavi、P. Kairouz 和 A. T. Suresh。联邦学习中的差分隐私洗牌模型。载于人工智能与统计国际会议，第 2521–2529 页。PMLR，2021年。.[54] Y. Han、A. Ozg¨ur 和 T. Weissman。通信约束下分布式参数估计的几何下界。载于学习理论会议，第 3163–3188 页。PMLR，2018年。[55] R. Hu、Y. Gong 和 Y. Guo。结合稀疏化增强隐私和自适应优化的联邦学习。*arXiv* 预印本 *arXiv:2008.01558*，2020年。[56] Z. Huang、Y. Qiu、K. Yi 和 G. Cormode。多方差分隐私下的频率估计：单轮与流式处理。*VLDB*基金会会刊，15(10):2058–2070，2022年6月。[57] P. Kairouz、K. Bonawitz 和 D. Ramage。本地隐私下的离散分布估计。载于第*33*届国际机器学习会议论文集，第 48 卷，第 2436–2444 页，美国纽约州纽约，2016年6月20–22日。

[58] P. Kairouz、Z. Liu 和 T. Steinke。用于安全聚合联邦学习的分布式离散高斯机制。arXiv 预印本 arXiv:2102.06387，2021年。[59] P. Kairouz、H. B. McMahan、B. Avent、A. Bellet、M. Bennis、A. N. Bhagoji、K. Bonawitz、Z. Charles、G. Cormode、R. Cummings 等。联邦学习的进展与开放问题。arXiv 预印本 arXiv:1912.04977，2019年。[60] P. Kairouz、H. B. McMahan、B. Avent、A. Bellet、M. Bennis、A. N. Bhagoji、K. Bonawitz、Z. Charles、G. Cormode、R. Cummings 等。联邦学习的进展与开放问题。《机器学习基础与趋势》，14(1–2):1–210，2021年。[61] B. Kashin。若干有限维集合及光滑函数类的截面（俄语）。《苏联科学院通报》，41:334–351，1977年。[62] S. P. Kasiviswanathan、H. K. Lee、K. Nissim、S. Raskhodnikova 和 A. Smith。我们能以隐私方式学到什么？SIAM 计算期刊，40(3):793–826，2011年。[63] J. Koneˇcn`y、H. B. McMahan、F. X. Yu、P. Richt´arik、A. T. Suresh 和 D. Bacon。联邦学习：提升通信效率的策略。arXiv 预印本 arXiv:1610.05492，2016 年。[64] A. Korolova、K. Kenthapadi、N. Mishra 和 A. Ntoulas。以隐私方式发布搜索查询和点击数据。载于《第18届国际万维网会议论文集》，第 171–180 页，2009年。[65] N. Li、W. Qardaji 和 D. Su。关于抽样、匿名化和差分隐私，或者说，k-匿名化遇上差分隐私。载于《第7届 ACM 信息、计算与通信安全研讨会论文集》，第 32–33 页，2012年。[66] Y. Lyubarskii 和 R. Vershynin。不确定性原理与矢量量化。《IEEE信息论汇刊》，56(7):3491–3501，2010年。[67] H. B. McMahan、E. Moore、D. Ramage、S. Hampson 和 B. Arcas。基于去中心化数据的深度网络通信高效学习（2016）。arXiv 预印本 arXiv:1602.05629，2016年。[68] I. Mironov。Rényi 差分隐私。载于《2017年 IEEE 第30届计算机安全基础研讨会（CSF）》，第 263–275 页。IEEE，2017年。[69] T. T. Nguyˆen、X. Xiao、Y. Yang、S. C. Hui、H. Shin 和 J. Shin。利用本地差分隐私收集并分析智能设备用户的数据，2016年。[70]M. Safaryan、E. Shulgin 和 P. Richt´arik。分布式与联邦学习中通信压缩的不确定性原理及最优压缩器探索。arXiv 预印本 arXiv:2002.08958，2020年。[71] A. Shah、W.-N. Chen、J. Balle、P. Kairouz 和 L. Theis。本地差分隐私机制的最优压缩。载于《人工智能与统计国际会议》，第 7680–7723 页。PMLR，2022年。[72] C. Studer、W. Yin 和 R. G. Baraniuk。具有最小 ℓ_∞-范数的信号表示。载于《2012年第50届 Allerton 通信、控制与计算会议（Allerton）》，第 1270–1277 页。IEEE，2012年。[73] A. T. Suresh、F. X. Yu、S. Kumar 和 H. B. McMahan。有限通信下的分布式均值估计。载于《第34届国际机器学习会议论文集》第70卷（ICML'17），第 3329–3337 页。JMLR.org，2017年。[74] R. Vershynin。高维概率：数据科学中的应用导论，第47卷。剑桥大学出版社，2018年。[75] T. Wang、J. Zhao、X. Yang 和 X. Ren。本地差分隐私数据收集与分析。arXiv 预印本 arXiv:1906.01777，2019年。

[76] J. Wangni、J. Wang、J. Liu 和 T. Zhang。用于实现通信高效分布式优化的梯度稀疏化。载于神经信息处理系统进展，第 1299–1309 页，2018年。[77] S. L. Warner。随机响应：一种消除回避作答偏差的调查技术。美国统计学会会刊，60(309):63–69，1965年。[78] W. Wen、C. Xu、F. Yan、C. Wu、Y. Wang、Y. Chen 和 H. Li。Terngrad：用于减少分布式深度学习通信开销的三值梯度。载于神经信息处理系统进展，第 1509–1519 页，2017年。[79] M. Ye 和 A. Barg。在本地差分隐私下进行离散分布估计的最优方案。载于*2017*年 *IEEE*国际信息论研讨会 *(ISIT)*，第 759–763 页，2017年 6 月。[80] W. Zhu、P. Kairouz、B. McMahan、H. Sun 和 W. Li。采用差分隐私的联邦重频项发现。载于人工智能与统计国际会议，第 3837–3847 页。PMLR，2020年。[81] Y. Zhu 和 Y.-X. Wang。Poission 子采样 Rényi 差分隐私。载于国际机器学习会议，第 7634–7642 页。PMLR，2019年。

定理 4.1 的证明

显然，平均通信成本为 $d\cdot\gamma=b$ 比特。为计算 ℓ_2^2 估计误差，注意到

$$
\begin{aligned}
&\mathbb{E}\left[\|\hat{\mu}_{x^n}-\mu_{x^n}\|_2^2\right]\\
&=\sum_{j=1}^{d}\mathbb{E}\left[\left(\frac{1}{n\gamma}\sum_i x_i(j)\cdot Z_{i,j}+N(0,\sigma^2)-\frac{1}{n}\sum_i x_i(j)\right)^2\right]\\
&=\sum_{j=1}^{d}\frac{1}{n^2}\mathbb{E}\left[\left(\frac{1}{\gamma}\sum_i x_i(j)\cdot Z_{i,j}-\sum_i x_i(j)\right)^2\right]+d\sigma^2\\
&=\sum_{j=1}^{d}\frac{1}{n^2}\mathbb{E}\left[\left(\frac{1}{\gamma}\sum_i x_i(j)\cdot Z_{i,j}\right)^2\right]-\frac{1}{n^2}\left(\sum_i x_i(j)\right)^2+d\sigma^2\\
&=\sum_{j=1}^{d}\frac{1}{n^2}\mathbb{E}\left[\frac{1}{\gamma^2}\sum_i x_i^2(j)\cdot Z_{i,j}^2+\frac{1}{\gamma^2}\sum_{i\neq i'}x_i(j)x_{i'}(j)Z_{i,j}Z_{i',j}\right]-\frac{1}{n^2}\left(\sum_i x_i(j)\right)^2+d\sigma^2\\
&=\sum_{j=1}^{d}\frac{1}{n^2}\left(\frac{1}{\gamma}\sum_i x_i^2(j)+\sum_{i\neq i'}x_i(j)x_{i'}(j)\right)-\frac{1}{n^2}\left(\sum_i x_i(j)\right)^2+d\sigma^2\\
&=\sum_{j=1}^{d}\frac{1}{n^2}\left(\frac{1}{\gamma}-1\right)\left(\sum_i x_i^2(j)\right)+d\sigma^2\\
&\le\frac{dc^2}{n\gamma}+d\sigma^2,
\end{aligned}
$$

由此得到不等式 (2)。接下来，我们分析算法 1 的隐私。首先给出以下两个关于子采样和高斯机制的引理：

引理 A.1 ([65, 81])**.** 若 $\mathcal{M}$ 满足 (ε,δ)-差分隐私，则应用 $\mathcal{M}\circ\mathsf{PoissonSample}$ 的 $\mathcal{M}'$ 满足 (ε',δ')-差分隐私，其中$\varepsilon'=\log(1+\gamma\left(e^{\varepsilon}-1\right))$，且 $\delta'=\gamma\delta$。

引理 A.2 ([15])**.** 对于任意 $\varepsilon,\delta\in(0,1)$，具有 $\sigma^2:=\frac{\Delta^2 2\log(1.25/\delta)}{\varepsilon^2}$的高斯输出扰动机制满足 (ε,δ)-差分隐私，其中 Δ 是目标函数的 ℓ_2 敏感度。

现在，我们利用上述两个引理分析算法 1 的逐坐标隐私泄露。为简洁起见，我们改为分析 $x_i(j)$之和（并在最后一步将其归一化）。设 $S_j(x^n):=\sum_{i=1}^n(x_i(j))$，则显然 $S_j(x^n)$ 的敏感度为 c，因此由引理 A.2 可知，若设 $\sigma_1^2=\frac{2c^2\log(1.25/\delta_1)}{\varepsilon_1^2}$（假设 $\varepsilon_1<1$），则 $S_j(x^n)+N(0,\sigma_1^2)$ 满足 (ε_1,δ_1)-差分隐私。接下来，若在计算总和之前进行子采样，即，

$$
S_j\circ\mathsf{PoissonSample}_\gamma(x^n):=\sum_{i=1}^{n}x_i(j)Z_{i,j},
$$

其中 $Z_{i,\ j}\overset{\text{独立同分布}}{\sim}$ 伯努利分布$(1/\gamma)$，如算法 1 中所定义，则根据引理 A.1，

$$
S_j\circ\mathsf{PoissonSample}_\gamma(x^n)+N(0,\sigma_1^2)
$$

满足 $(\varepsilon_2,\ \delta_2)$-差分隐私，其中 $\varepsilon_2:=\log\left(1+\gamma(e^{\varepsilon_1}-1)\right)\ =\ C_1\gamma\varepsilon_1$(因为我们假设 $\epsilon_1<1$)，且 $\delta_2:=\gamma\delta_1$。等价地，我们有

$$
\begin{cases}\varepsilon_1=\tilde{C}_1\frac{1}{\gamma}\varepsilon_2\\ \delta_1=\frac{1}{\gamma}\delta_2.\end{cases}\tag{9}
$$

现在，由于我们已确定逐坐标隐私泄露，我们应用以下组合定理来计算总隐私预算。

定理 A.3。对于任意 $\varepsilon > 0$、$\delta \in [0,1]$ 和 $\tilde{\delta} \in (0,1]$，类 (ε, δ)- 差分隐私机制在 d 重自适应组合下满足 $(\tilde{\varepsilon}_{\tilde{\delta}}, d\delta+\delta)$- 差分隐私，其中

$$\tilde{\varepsilon}_{\tilde{\delta}} = d\varepsilon\left(e^{\varepsilon}-1\right) + \varepsilon\sqrt{2d\log(1/\tilde{\delta})}.$$

根据定理 A.3，算法 1 满足 $(\varepsilon,\ \delta)$-差分隐私，其条件为

$$\varepsilon = d\varepsilon_2(e^{\varepsilon_2}-1) + \varepsilon_2\sqrt{2d\log(1/\tilde{\delta})}, \tag{10}$$

且 $\delta = d\delta_2 + \delta$（其中 δ 是一个可优化的自由参数）。

因此，对于预先指定的（总）隐私预算 $(\varepsilon,\ \delta)$，我们将参数设置如下。令 $\tilde{\delta} = \frac{\delta}{2}$ 和 $\delta_1 = \frac{1}{\gamma}\delta_2 = \frac{1}{2d\gamma}\delta$。令 $\varepsilon_2 \le 1$，使得 $e^{\varepsilon}_2 - 1 \le 2\varepsilon_2$ 成立。于是，由 (10) 可知算法 1 是

$$\varepsilon = 2d\varepsilon_2^2 + \varepsilon_2\sqrt{2d\log(1/\tilde{\delta})} \ge d\varepsilon_2(e^{\varepsilon_2}-1) + \varepsilon_2\sqrt{2d\log(1/\tilde{\delta})}.$$

对上述关于 ε_2 的二次（不）等式求解，可得

$$\varepsilon_2 = \min\left(1, \frac{-\sqrt{2d\log(2/\delta)} + \sqrt{2d\log(2/\delta) + 8\varepsilon d}}{4d}\right) = O\left(\min\left(1, \frac{\varepsilon}{\sqrt{d\left(\log(1/\delta)+\varepsilon\right)}}\right)\right).$$

因此，我们设 $\varepsilon_1 = \frac{\tilde{C}_1}{\gamma}\varepsilon_2 = O\left(\min\left(1, \frac{\varepsilon}{\gamma\sqrt{d(\log(1/\delta)+\varepsilon)}}\right)\right)$（注意，我们要求 $\varepsilon_1 = O(1)$，以使 (9) 成立）。

将 $(\varepsilon_1,\ \delta_1)$ 代入 σ_1^2，得到

$$\sigma_1^2 \coloneqq \frac{2c^2\log(1.25/\delta_1)}{\varepsilon_1^2} = \Omega\left(\max\left(c^2\log(d/\delta), \frac{\gamma^2c^2d(\log(1/\delta)+\varepsilon)\log(d/\delta)}{\varepsilon^2}\right)\right).$$

最后，由于我们关注的是估计（子采样后的）均值，而非总和，因此我们将隐私求和归一化为

$$\hat{\mu}_j(x^n) = \frac{1}{n\gamma}\left(S_j \circ \mathsf{PoissonSample}_{\gamma}(x^n) + N(0,\sigma_1^2)\right) = \frac{1}{n\gamma}S_j \circ \mathsf{PoissonSample}_{\gamma}(x^n) + N(0,\sigma^2),$$

其中

$$\sigma^2 = O\left(\max\left(\frac{c^2\log(d/\delta)}{n^2\gamma^2}, \frac{c^2d(\log(1/\delta)+\varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right).$$

将上面的 σ^2 和 $\gamma = d/b$ 代入，即可得到定理 4.1 中所需的准确度。 □

由于我们将重复使用上述结果，现将其总结为以下引理：

引理 A.4. 设 $f_i\colon\ \mathbb{R}^{d\times m} \mapsto \mathbb{R}^D$ 对于 $i = 1$、...、B 是 n 函数，其敏感度上界为 Δ（其中，输入数量 m 可以是随机变量）。则

$$\left(f_1 \circ \mathsf{PoissonSample}_{\gamma}(x^n) + N(0,\sigma^2), ..., f_B \circ \mathsf{PoissonSample}_{\gamma}(x^n) + N(0,\sigma^2)\right)$$

满足(ε, δ)-差分隐私，如果

$$\sigma^2 \ge O\left(\max\left(\Delta^2\log(B/\delta), \frac{\gamma^2\Delta^2B(\log(1/\delta)+\varepsilon)\log(B/\delta)}{\varepsilon^2}\right)\right).$$

B 定理 4.4 的证明

要证明定理 4.4，只需证明以下 ℓ_∞ 版本：

定理 B.1. 设 $x_1, ..., x_n \in \{-c, c\}^d$, $d' =$最小值 $\left(nb, \quad \underline{\frac{n^2\varepsilon^2}{1/\delta + \varepsilon (\log()) \log(d/\delta)}}\right)$, 且

$$\sigma^2 = O\left(\frac{c^2 \log(1/\delta)}{n^2\gamma^2} + \frac{c^2 d'(\log(d'/\delta) + \varepsilon)\log(d'/\delta)}{n^2\varepsilon^2}\right). \tag{11}$$

那么，算法 2 是(ε, δ)-差分隐私，并在 μ 上产生一个无偏估计量。此外，平均每客户端通信成本为 $\gamma d' = b$ 比特，且 ℓ_2^2 估计误差至多为

$$O\left(c^2 d^2 \log\left(\frac{d}{\delta}\right) \max\left(\frac{1}{nb}, \frac{(\log(1/\delta) + \varepsilon)}{n^2\varepsilon^2}\right)\right). \tag{12}$$

稍微滥用一下记号，令 $\mu_{\mathcal{J}} \in \mathbb{R}^d$ 满足

$$\mu_{\mathcal{J}}(j) = \begin{cases} 0, & \text{if} j \notin \mathcal{J} \\ \frac{d\mu_j}{d'}, & \text{else.} \end{cases}$$

注意，若 $\mathcal{J}$ 是均匀随机选取的，则 $\mu_{\mathcal{J}}$ 是 μ 的无偏估计。因此， ℓ_2^2 误差可由下式控制:

$$\begin{aligned}
\mathbb{E}\left[\|\mu - \hat{\mu}\|_2^2\right] &\overset{(a)}{=} \mathbb{E}\left[\|\mu - \mu_{\mathcal{J}}\|_2^2\right] + \mathbb{E}\left[\|\mu_{\mathcal{J}} - \hat{\mu}\|_2^2\right] \\
&\overset{(b)}{\leq} \mathbb{E}\left[\|\mu - \mu_{\mathcal{J}}\|_2^2\right] + \frac{d^2}{d'^2} O\left(\max\left(\frac{d'^2 c^2}{nb}, \frac{d'^3 c^2 \log(d/\delta)}{n^2 b^2}, \frac{c^2 d'^2 (\log(1/\delta) + \varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right) \\
&= \mathbb{E}\left[\|\mu - \mu_{\mathcal{J}}\|_2^2\right] + O\left(\max\left(\frac{d^2 c^2}{nb}, \frac{d^2 d' c^2 \log(d/\delta)}{n^2 b^2}, \frac{c^2 d^2 (\log(1/\delta) + \varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right) \\
&\overset{(c)}{\leq} \frac{d^2 c^2}{d'} + O\left(\max\left(\frac{d^2 c^2}{nb}, \frac{d^2 d' c^2 \log(d/\delta)}{n^2 b^2}, \frac{c^2 d^2 (\log(1/\delta) + \varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right),
\end{aligned}$$

其中，(a) 成立是因为 $\mu_{\mathcal{J}}$ 是 μ 的无偏估计，且在给定 $\mathcal{J}$ 的条件下，$\hat{}\mu$ 是 $\mu_{\mathcal{J}}$ 的无偏估计；(b) 根据定理 4.1 得出；(c) 则基于以下事实成立:

$$\mathbb{E}\left[\|\mu - \mu_{\mathcal{J}}\|_2^2\right] \leq \sum_{j \in \mathcal{J}} \mu_{\mathcal{J}}(j)^2 + \sum_{j \in [d]} \mu_j^2 \leq \frac{d^2 c^2}{d'} + dc^2 \leq \frac{2d^2 c^2}{d'}.$$

因此，令 $d' =$min $\left(nb, \quad \underline{\frac{n^2\varepsilon^2}{1/\delta + \varepsilon (\log()) \log(d/\delta)}}\right)$，即可确保 (c) 中第一项始终小于第二项，而第二项可简化如下:

$$\begin{aligned}
&O\left(c^2 d^2 \max\left(\frac{1}{nb}, \frac{d' \log(d/\delta)}{n^2 b^2}, \frac{(\log(1/\delta) + \varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right) \\
&\leq O\left(c^2 d^2 \max\left(\frac{1}{nb}, \frac{nb \log(d/\delta)}{n^2 b^2}, \frac{(\log(1/\delta) + \varepsilon)\log(d/\delta)}{n^2\varepsilon^2}\right)\right) \\
&\leq O\left(c^2 d^2 \log(d/\delta) \max\left(\frac{1}{nb}, \frac{(\log(1/\delta) + \varepsilon)}{n^2\varepsilon^2}\right)\right).
\end{aligned}$$

最后，应用 Kashin 表示的同一技巧，我们可以将 ℓ_∞ 几何变换为 ℓ_2（类似于命题 4.3），从而证明定理 4.4。□

C 定理 5.1 的证明

令 $\pi := \frac{1}{n}\sum_i x_i$ 和 $\pi^{(\ell)}$ 按照 $\ell \in [B]$ 中定义 $x_i^{(\ell)}$ 的相同方式定义。我们的目标是对所有 $\ell \in [2^{b-1}]$ 和 $j \in [B]$, 给出$\left|\pi^{(\ell)}(j) - \hat{}\pi^{(\ell)}(j)\right|$的上界。

为此，令 $y^{(\ell)} \coloneqq H_B \cdot \pi^{(\ell)}$ （因此有 $\pi^{(\ell)} = \frac{1}{B} H_B \cdot y^{(\ell)}$）。于是我们有

$$\begin{aligned}\mathbb{E}\left[\left|\pi^{(\ell)}(j) - \hat{\pi}^{(\ell)}(j)\right|\right] &\overset{\text{(a)}}{\leq} \sqrt{\mathbb{E}\left[\left(\pi^{(\ell)}(j) - \hat{\pi}^{(\ell)}(j)\right)^2\right]} \\ &= \sqrt{\mathbb{E}\left[\left(\frac{1}{B} H_B \cdot \left(y^{(\ell)} - \hat{y}^{(\ell)}\right)(j)\right)^2\right]}. \end{aligned} \tag{13}$$

接下来注意到，由于子采样步骤，对于所有 $\ell \in [2^{b-1}]$ 和 $j \in [B]$,

$$\hat{y}^{(\ell)}(j) = \frac{B}{n} \sum_{i=1}^{n} \langle (H_B)_j, x_i^{(\ell)} \rangle \cdot Z_{ij} + N(0, \sigma^2),$$

其中回顾一下， $Z_{ij} \overset{\text{独立同分布}}{\sim} \mathsf{Ber}(1/B)$。因此，$\hat{}y^{(\ell)}(j)$是 $y^{(\ell)}(j)$的无偏估计量。此外，由于我们在算法 3 中独立地选择 Z_{ij}，对于不同的 j，$\hat{}y^{(\ell)}(j)$相互独立，因此有

$$\begin{aligned}\mathbb{E}\left[\left(\hat{y}^{(\ell)}(j) - y^{(\ell)}(j)\right)^2\right] &= \mathsf{Var}\left(\hat{y}^{(\ell)}(j)\right) \\ &= \sigma^2 + \frac{B^2}{n^2} \sum_{i=1}^{n} \langle (H_B)_j, x_i^{(\ell)} \rangle^2 \mathsf{Var}\left(Z_{ij}\right) \\ &\leq \sigma^2 + \frac{B}{n^2} \sum_{i=1}^{n} \langle (H_B)_j, x_i^{(\ell)} \rangle^2 \\ &= \sigma^2 + \frac{B}{n^2} \underbrace{\sum_{i=1}^{n} \mathbb{1}_{\{x_i \in \ell\text{-th chunk}\}}}_{\coloneqq C_\ell}, \end{aligned} \tag{14}$$

并且对于所有 $j \neq j'$

$$\mathbb{E}\left[\left(\hat{y}^{(\ell)}(j) - y^{(\ell)}(j)\right) \cdot \left(\hat{y}^{(\ell)}(j') - y^{(\ell)}(j')\right)\right] = 0. \tag{15}$$

因此，我们继续对式 (13)进行如下界定:

$$\begin{aligned}\sqrt{\mathbb{E}\left[\left(\frac{1}{B} H_B \cdot \left(y^{(\ell)} - \hat{y}^{(\ell)}\right)(j)\right)^2\right]} &= \sqrt{\frac{1}{B^2}\mathbb{E}\left[\langle (H_B)_j, \left(\hat{y}^{(\ell)} - y^{(\ell)}\right)\rangle^2\right]} \\ &= \sqrt{\frac{1}{B^2}\mathbb{E}\left[\left(\sum_{k=1}^{B} (H_B)_{jk} \cdot \left(\hat{y}^{(\ell)}(k) - y^{(\ell)}(k)\right)\right)^2\right]} \\ &\overset{\text{(a)}}{=} \sqrt{\frac{1}{B^2}\mathbb{E}\left[\sum_{k=1}^{B} \left(\hat{y}^{(\ell)}(k) - y^{(\ell)}(k)\right)^2\right]} \\ &\overset{\text{(b)}}{=} \sqrt{\frac{C_\ell}{n^2} + \frac{\sigma^2}{B}} \\ &\overset{\text{(c)}}{\leq} \sqrt{\frac{1}{n} + \frac{\sigma^2}{B}}, \end{aligned}$$

其中，(a)成立是因为 H_B 的每个分量取值于 $\{-1, 1\}$，且根据式 (15)；(b)成立是因为式 (14)；(c)成立是因为对于所有 ℓ， $C_\ell \leq n$。

最后，为了界定 ℓ_2^2 误差，请注意上述分析保证了

$$\mathbb{E}\left[\left(\pi^{(\ell)}(j) - \hat{\pi}^{(\ell)}(j)\right)^2\right] \leq \frac{C_{\ell(j)}}{n^2} + \frac{\sigma^2}{B},$$

其中 $\ell(j) \in [2^{b-1}]$ 是包含 j 的区块索引。因此，对 $j \in [d]$ 求和后，我们必须有 ve

$$\mathbb{E}\left[\left\|\pi^{(\ell)} - \hat{\pi}^{(\ell)}\right\|_2^2\right] \leq \sum_{j=1}^{d} \frac{C_{\ell(j)}}{n^2} + \frac{d\sigma^2}{B} = \frac{B}{n} + \frac{d\sigma^2}{B},$$

因为

$$\sum_j C_{\ell(j)} = \sum_{\ell=1}^{2^{b-1}} \sum_{j' \in \ell\text{-th chunk}} \sum_{i=1}^{n} \mathbb{1}_{\{i \in \ell-\text{th chunk}\}} = B \sum_{\ell=1}^{2^{b-1}} \sum_{i=1}^{n} \mathbb{1}_{\{i \in \ell-\text{th chunk}\}} = B \cdot n.$$

□

D 定理 5.2 的证明

设 $f_j(x^n) := (\pi^{(1)}(j) ..., \pi^{(2^{b-1})}(j))$，其中 $j = 1, ..., B$。那么， f_j 的 ℓ_2 敏感度为 $\Delta = \frac{B}{n}$。设采样率为 $\gamma = \frac{1}{B}$，根据引理 A.4，证明得证。□

E 洗牌 SQKR 算法

算法 4 洗牌 SQKR

输入：用户数据 $x_1, \ldots, x_n$，本地差分隐私参数 ε_0，通信参数 b_0, T输出：均值估计量 $\hat{}\mu$对于轮次 $k \in [T]$，执行以下操作：对于用户 $i \in [n]$，执行以下操作：从 $[d]$ 中独立同分布地采样 $s(i, 1) \ldots, s(i, b_0)$ ∼从 Unif$[d]$ 中采样 $Z \sim$伯努利分布 $\left(\frac{e^{\varepsilon_0}}{e^{\varepsilon_0}+2^{b_0}-1}\right)$ 如果 Z=1，则将 $Y(i, 1) \ldots, Y(i, b_0)$ 设置为 $\leftarrow x_i(s(i, 1)) \ldots, x_i(s(i, b_0))$否则，从 Unif $\{-c, c\}$ 中独立同分布地采样 $Y(i, 1) \ldots, Y(i, b_0)$ ∼结束判断将 $Y(i, 1) \ldots, Y(i, b_0)$ 和 $s(i, 1) \ldots, s(i, b_0)$ 发送给洗牌器结束循环洗牌器从 Unif $\{f$ 中采样一个置换 $\pi \sim :$ $[n] \to [n]$ 双射$\}$对于 $j \in [b_0]$，执行以下操作：洗牌器将 $Y(\pi(1)\ j) \ldots, Y(\pi(n)\ j)$ 和 $s(\pi(1)\ j) \ldots, s(\pi(n)\ j)$ 发送给服务器结束循环$\hat{}\mu^{(k)} \leftarrow \frac{d}{nb_0} \frac{e^{\varepsilon_0}+2^{b_0}-1}{e^{\varepsilon_0}-1} \sum_{i=1}^{n} \sum_{j=1}^{b_0} Y(\pi(i)\ j) e_{s(\pi(i),j)}$结束循环返回 $\hat{}\mu := \frac{1}{T} \sum_{k=1}^{T} \hat{}\mu^{(k)}$

F 定理 6.4 的证明

算法 4 的每一轮 $x^n \mapsto \hat{}\mu^{(k)}$ 都实现了 [32]，中的私有硬币 SQKR 方案，达到引理 6.3 中所述的通信开销和误差。

引理 *F.1*（*SQKR* [32]）。对于所有 $\varepsilon_0 > 0$、$b_0 > 0$，算法 *4* 中的随机映射 $x_i \mapsto y(i, 1) \ldots, y(i, b_0)\ s(i, 1) \ldots, s(i, b_0)$ 满足 $(\varepsilon_0, 0)$- 本地差分隐私，其输出可使用 b_0 *log(d)* 比特进行通信，并且根据 $y(i, 1) \ldots, y(i, b_0)\ s(i, 1) \ldots, s(i, b_0)$ 计算得到的 $\hat{}\mu^{(k)}$ 是一个无偏估计量，满足

$$\max_{x^n} \mathbb{E}\left[\left\|\mu\left(x^n\right) - \hat{\mu}^{(k)}\left(x^n\right)\right\|_2^2\right] = O\left(\frac{c^2 d}{n \min\left(\varepsilon_0^2, \varepsilon_0, b_0\right)}\right). \tag{16}$$

现在，我们将刻画在满足隐私与通信约束的参数一般取值下，算法 4 的错误性能。

命题 F.2。 对于任意的 $\varepsilon > 0$、$b > 0$、$n > 0$，无论如何选择

$$\delta_1 \in \left(e^{-n}, 1\right] \tag{17}$$

$$\delta_2 \in (0, 1], \tag{18}$$

都存在一组参数 ε_0、b_0、T，使得算法 4 满足$(\varepsilon,\ T\delta_1 + \delta_2)$-差分隐私，使用的通信量不超过 b 比特，并且

$$\max_{x^n} \mathbb{E}\left[\|\mu - \hat{\mu}\|_2^2\right] = O\left(\max\left(\frac{c^2 d \log(d) b_0}{nb}, \frac{c^2 d \log(1/\delta_1)\left(\log(1/\delta_2) + \varepsilon\right)}{n^2\varepsilon^2}\right)\right). \tag{19}$$

证明。 对于任意选择的

$$b_0 < \log\left(\frac{n}{16\log(2)}\right), \tag{20}$$

只需选择

$$T = \left\lfloor \frac{b}{(\log_2(d) + 1) b_0} \right\rfloor \tag{21}$$

$$\varepsilon_0 = O\left(\min\left(1, \frac{\varepsilon\sqrt{n}}{\sqrt{T\log(1/\delta_1)\left(\log(1/\delta_2) + \varepsilon\right)}}\right)\right). \tag{22}$$

由于发送 $y(i,1)\ldots, y(i,b_0)$ 需要 b_0 比特，发送每个 $s(i,1)\ldots, s(i,b_0)$ 需要 $\log_2(d)$ 比特，且这一操作要执行 T 次，因此根据 T 的选择，算法 4 使用少于 b 比特显然成立。

应用引理 F.1，根据构造，从每个 x_i 到 $y(i,1)\ldots, y(i,b_0)$ 的映射满足 $(\varepsilon_0, 0)$-本地差分隐私。根据假设

$$\delta_1 > e^{-n/16e} > e^{-n}, \tag{23}$$

该不等式

$$1 < \log\left(\frac{n}{16\log(2/\delta_1)}\right) \tag{24}$$

成立。于是，选择

$$\varepsilon_0 \le 1 \tag{25}$$

也满足 $\varepsilon_0 \le \log\left(\underline{{}_{16}\ {}^{n}\log(2/\delta)}\right)$，因此根据引理 6.1，映射 $x^n \mapsto \hat{\mu}^{(k)}$ 满足 $(\varepsilon_1, \delta_1)$-差分隐私。其中

$$\varepsilon_1 = O\left(\frac{\varepsilon_0\sqrt{\log(1/\delta_1)}}{\sqrt{n}}\right). \tag{26}$$

由于算法 4 的输出是 $\left(\hat{\mu}^{(1)}, \ldots, \hat{\mu}^{(T)}\right)$ 的函数，根据 A.3，只需满足

$$\varepsilon_1 = O\left(\min\left(1, \frac{\varepsilon}{\sqrt{T(\log(1/\delta_2) + \varepsilon)}}\right)\right) \tag{27}$$

使算法 4 满足 $(\varepsilon, T\delta_1 + \delta_2)$-差分隐私。第一个不等式由 $\delta_1 > e^{-n}$ 的假设和对 $\varepsilon_0 = O(1)$ 的选择得出，第二个不等式则由对

$$\varepsilon_0 = O\left(\frac{\varepsilon\sqrt{n}}{\sqrt{T\log(1/\delta_1)\left(\log(1/\delta_2) + \varepsilon\right)}}\right). \tag{28}$$

由于 $\varepsilon_0 \leq 1 \leq b$，我们有 $\min(\varepsilon_0^2, \varepsilon_0, b) = \varepsilon_0^2$。应用引理 F.1，

$$\max_{x^n} \mathbb{E}\left[\|\mu - \hat{\mu}\|_2^2\right] = \frac{1}{T} \max_{x^n} \mathbb{E}\left[\left\|\mu - \hat{\mu}^{(1)}\right\|_2^2\right] \tag{29}$$

$$= O\left(\frac{d}{Tn\varepsilon_0^2}\right) \tag{30}$$

$$= O\left(\max\left(\frac{d}{Tn}, \frac{d\log(1/\delta_1)\left(\log(1/\delta_2) + \varepsilon\right)}{n^2\varepsilon^2}\right)\right). \tag{31}$$

代入 T 的取值即可得到所需结果。 □

为证明定理 6.4，只需选择

$$b_0 = 1 \tag{32}$$

$$\delta_1 = \frac{\delta}{2T} \tag{33}$$

$$\delta_2 = \frac{\delta}{2}, \tag{34}$$

根据 (20)，这要求 $n > 16e\log(2) \approx 30.14$，然后应用前一个命题。

洗牌 SQKR 的 G R´enyi-差分隐私

我们可以使用以下结果来保证算法 4 的 Rényi 差分隐私（RDP）。

引理 G.1 ([44] 推论 4.3)。设对每个 $i \in [n]$，$\mathcal{M}_i$ 都是一个独立的$(\varepsilon_0, 0)$-本地差分隐私机制，满足$\varepsilon_0 \leq 1$，且 π 是 $[n]$ 的一个随机排列。那么对于任意 $\alpha < {}_{16\varepsilon_0}{}^{n}\exp(\varepsilon_0)$，该机制

$$\mathcal{S} : (x_1, \ldots, x_n) \mapsto \left(\mathcal{M}_1\left(x_{\pi(1)}\right), \ldots, \mathcal{M}_n\left(x_{\pi(n)}\right)\right)$$

是 $(\varepsilon(\alpha)\ \delta)$-*Rényi* 差分隐私，其中

$$\varepsilon(\alpha) = O\left(\alpha\left(1 - e^{-\varepsilon_0}\right)^2 \frac{e^{\varepsilon_0}}{n}\right). \tag{35}$$

应用引理 F.1，根据构造，从每个 x_i 到 $y(i,1) \ldots, y(i,b_0)$ 的映射满足 $(\varepsilon_0, 0)$-本地差分隐私。根据引理 G.1，映射 $x^n \mapsto \hat{}\mu^{(k)}$ 满足 (ε_1, α)-Rényi 差分隐私，其中

$$\varepsilon_1 = O\left(\alpha\left(1 - e^{-\varepsilon_0}\right)^2 \frac{e^{\varepsilon_0}}{n}\right) \tag{36}$$

根据组合，算法 4 满足 $(T\varepsilon_1, \alpha)$-Rényi 差分隐私。