Universal Exact Compression of Differentially Private Mechanisms

Yanxiao Liu[1] Wei-Ning Chen[2] Ayfer Özgür[2] Cheuk Ting Li[1]

yanxiaoliu@link.cuhk.edu.hk {wnchen, aozgur}@stanford.edu ctli@ie.cuhk.edu.hk

[1]The Chinese University of Hong Kong [2]Stanford University

Introduction

Local differential privacy (DP) [1].

Local randomizer $\mathcal{A}:\mathcal{X}\to\mathcal{Z}$ with distribution $P_{Z|X}$ satisfies (ε,δ)-local DP if for any $x,x'\in\mathcal{X}$ and measurable set $\mathcal{S}\subseteq\mathcal{Z}$,

$$\Pr(Z\in\mathcal{S}|X=x)\le e^{\varepsilon}\cdot\Pr(Z\in\mathcal{S}|X=x')+\delta.$$

Compression of DP mechanisms.

Objective: Compress DP mechanisms exactly (i.e., $Z\sim P_{Z|X}$) to near-optimal sizes, while ensuring privacy guarantees.

Prior works:

· [2-5]: Compress ε-local DP mechanism **approximately**.

· [6,7]: Dithered quantization tools ensure a correct simulated distribution, but only for additive noise mechanisms.

Poisson Functional Representation (PFR) [8]

Let $(T_i)_i$ be a Poisson process with rate 1, independent of $Z_i \overset{\text{i.i.d.}}{\sim} Q$. Then $(Z_i,T_i)_i$ is a Poisson process with intensity measure $Q\times\lambda_{[0,\infty)}$. Fix distribution P absolutely continuous w.r.t Q. Let

$$\tilde{T}_i\triangleq T_i\cdot\left(\frac{\mathrm{d}P}{\mathrm{d}Q}(Z_i)\right)^{-1}.$$

Theorem: $K\triangleq\arg\min_i\tilde{T}_i$ and $Z=Z_K$, then $Z\sim P$.

Our contributions: Poisson private representation, which is:

(a) **Exact**: simulates $P_{Z|X}$ exactly;

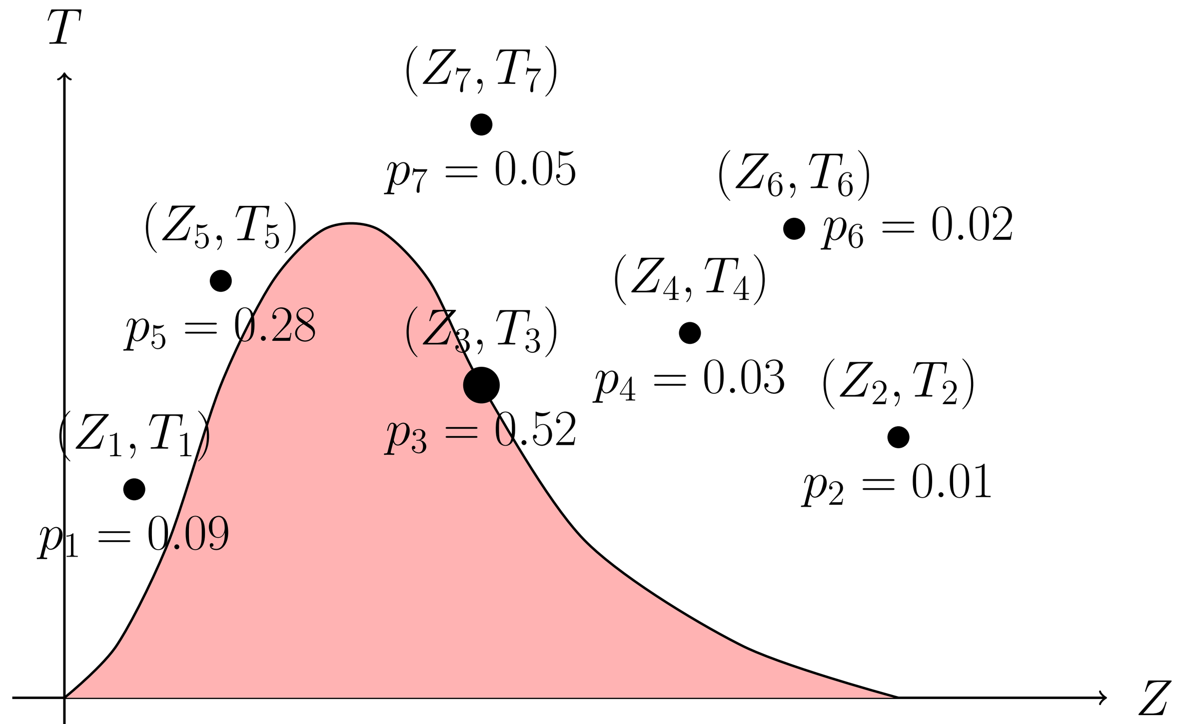
(b) **Universal**: simulates *any* DP mechanism;

(c) **Communication-efficient**: compresses $P_{Z|X}$ to

$$I(X;Z)+\log\big(I(X;Z)+1\big)+O(1)\text{ bits}.$$

(d) **Private**: ensures both local and central DP.

Poisson Private Representation ($p_k\triangleq\Pr(K=k)$):



https://github.com/cheuktingli/PoissonPrivateRepr

Poisson Private Representation (PPR)

Algorithm 1 (PPR).

Input: private $x\in\mathcal{X}$, (ε,δ)-local DP mechanism $P_{Z|X}$, reference distribution Q, parameter $\alpha>1$.

(a) Generate shared randomness between user and server

$$(Z_i)_{i=1,2,\dots}\overset{\text{i.i.d.}}{\sim}Q.$$

(b) The user knows $(Z_i)_i$, x, $P_{Z|X}$ and performs:

(1) Generate the Poisson process $(T_i)_i$ with rate 1.

(2) Compute $\tilde{T}_i\triangleq T_i\cdot\left(\frac{dP_{Z|X}(\cdot|x)}{dQ}(Z_i)\right)^{-1}$.

(3) Generate $K\in\mathbb{Z}_+$ with

$$\Pr(K=k)=\tilde{T}_k^{-\alpha}\Big/\left(\sum_{i=1}^{\infty}\tilde{T}_i^{-\alpha}\right).$$

(4) Compress and send K (e.g., by Elias delta code).

(c) The server, which knows $(Z_i)_i,K$, outputs $Z=Z_K$.

Exactness

The output Z of PPR follows $P_{Z|X}$ exactly.

Communication Efficiency

Thm 4.3: For PPR with $\alpha>1$, message K satisfies

$$\mathbb{E}[\log_2 K]\le D_{\mathsf{KL}}(P(\cdot|x)\|Q(\cdot))+\log_2(3.56)/\min((\alpha-1)/2,1).$$

K can be encoded by a prefix-free code with expected length $\approx D_{\mathsf{KL}}(P(\cdot|x)\|Q(\cdot))$ bits within a $\log$ gap. If $X\sim P_X$ is random, take $Q=P_Z$ and the expected length $\approx I(X;Z)$ (near-optimal).

Corollary 4.4: For $P_{Z|X}$ with ε-local DP, the compression size

$$\le\ell+\log_2(\ell+1)+2\ \text{(bits)},$$

where $\ell\triangleq\varepsilon\log_2 e+\log_2(3.56)/\min((\alpha-1)/2,1)$.

Privacy guarantees

❶ **Thm 4.5**: If the mechanism $P_{Z|X}$ is ε-DP, then PPR $P_{(Z_i)_i,K|X}$ with $\alpha>1$ is $2\alpha\varepsilon$-DP.

❷ **Thm 4.8**: If $P_{Z|X}$ is (ε,δ)-DP, then PPR $P_{(Z_i)_i,K|X}$ is $(\alpha\varepsilon+\tilde{\varepsilon},2(\delta+\tilde{\delta}))$-DP, for $\alpha>1$, $\tilde{\varepsilon}\in(0,1]$ and $\tilde{\delta}\in(0,1/3]$ s.t.

$$\alpha\le e^{-4.2}\tilde{\delta}\tilde{\varepsilon}^2/(-\ln\tilde{\delta})+1.$$

Remarks

- The exactness of PPR follows from the PFR [8].
- While the algorithm requires infinite samples, it can be reparametrized to terminate in finite steps.
- When $\alpha=\infty$, PPR reduces to PFR.

Application: Metric Privacy and Laplace Mechanism

For a mechanism $\mathcal{A}$ with $P_{Z|X}$ and a metric $d_{\mathcal{X}}$ over $\mathcal{X}$, it satisfies $\varepsilon\cdot d_{\mathcal{X}}$-privacy [9] if $\forall x,x'\in\mathcal{X}$, $\mathcal{S}\subseteq\mathcal{Z}$, we have

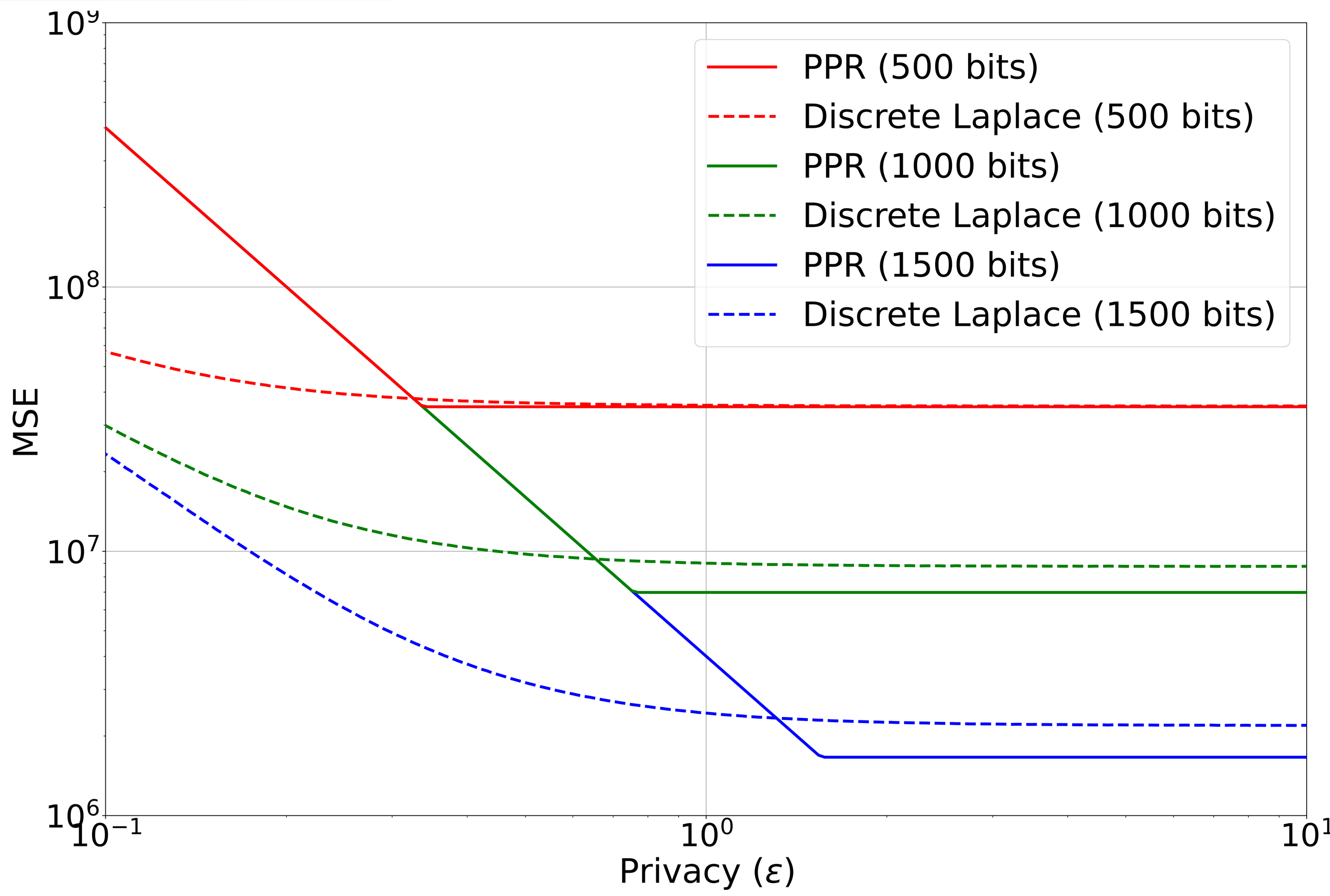
$$\Pr(Z\in\mathcal{S}\,|\,X=x)\le e^{\varepsilon\cdot d_{\mathcal{X}}(x,x')}\Pr(Z\in\mathcal{S}\,|\,X=x').$$

PPR-compressed Laplace mechanism:

For Laplace mechanism $P_{Z|X}$ with $X\in\{x\in\mathbb{R}^d\,|\,\|x\|_2\le C\}$ and proposal distribution $Q=\mathcal{N}(0,(\frac{C^2}{d}+\frac{d+1}{\varepsilon^2})\mathbb{I}_d)$, the output of PPR has MSE $\frac{d(d+1)}{\varepsilon^2}$, $2\alpha\epsilon\cdot d_{\mathcal{X}}$-privacy and compression size $\le\ell+\log_2(\ell+1)+2$ bits, where $\ell\triangleq$

$$\frac{d}{2}\log_2\left(\frac{2}{e}\left(\frac{C^2\varepsilon^2}{d}+d+1\right)\right)-\log_2\frac{\Gamma(d+1)}{\Gamma(\frac{d}{2}+1)}+\frac{\log_2(3.56)}{\min\{\frac{\alpha-1}{2},1\}}.$$

We compare with the discrete Laplace mechanism [9], $d=500$.



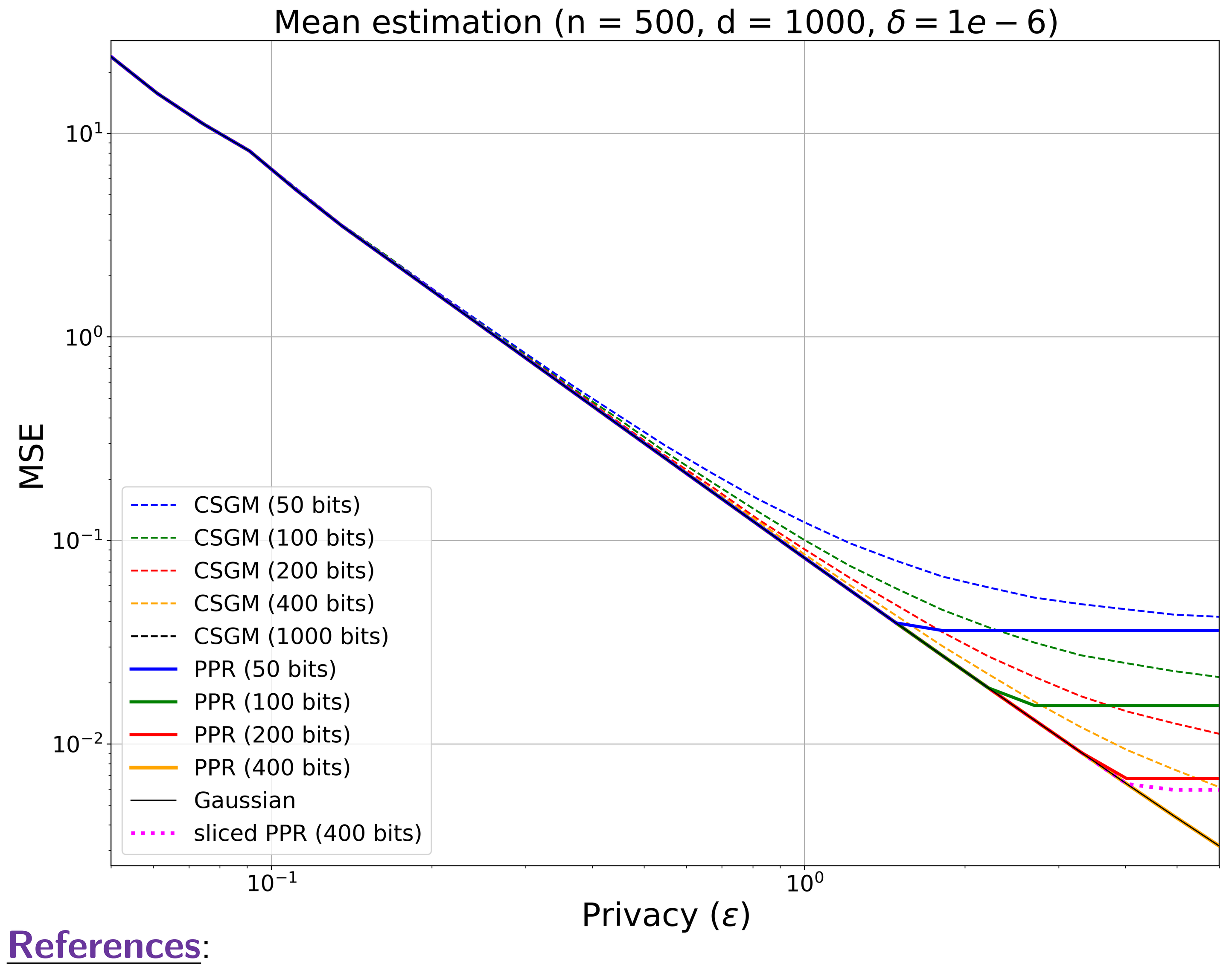
Distributed Mean Estimation

Consider n users, each with data $X_i\in\mathbb{R}^d$. They use **Gaussian mechanism** and send $Z_i\sim\mathcal{N}(X_i,\frac{\sigma^2}{n}\mathbb{I}_d)$ to server, where $\sigma\ge C\sqrt{2\ln(1.25/\delta)}/\varepsilon$. Server estimates mean as $\hat{\mu}(Z^n)=\frac{1}{n}\sum_i Z_i$. Using PPR to compress the Gaussian mechanism:

- $\hat{\mu}(Z^n)=\frac{1}{n}\sum_i Z_i$ is unbiased, has (ε,δ)-central DP.
- PPR satisfies $(2\alpha\sqrt{n}\varepsilon,2\delta)$-local DP for $\epsilon<1/\sqrt{n}$.
- The average per-user communication $\le\ell+\log_2(\ell+1)+2$ bits,

$$\ell:=\frac{d}{2}\log\left(\frac{n\varepsilon^2}{2d\log(1.25/\delta)}+1\right)+\frac{\log_2(3.56)}{\min\{(\alpha-1)/2,\,1\}}.$$

Compare to CSGM [10] on distributed mean estimation:



References:

[1] Kasiviswanathan, Lee, Nissim, Raskhodnikova and Smith, *"What can we learn privately?"* SIAM Journal on Computing, 2011.

[2] Feldman and Talwar, *"Lossless compression of efficient private local randomizers,"* ICML 2021.

[3] Shah, Chen, Balle, Kairouz and Theis, *"Optimal Compression of Locally Differentially Private Mechanisms,"* AISTATS 2022.

[4] Triastcyn, Reisser and Louizos, *"DP-REC: Private & Communication-Efficient Federated Learning,"* arXiv:2111.05454.

[5] Bassily and Smith, *"Local, private, efficient protocols for succinct histograms,"* STOC 2015.

[6] Hegazy, Leluc, Li and Dieuleveut, *"Compression with exact error distribution for federated learning,"* AISTATS 2024.

[7] Shahmiri, Ling and Li, *"Communication-efficient Laplace mechanism for differential privacy via random quantization,"* ICASSP 2024.

[8] Li and El Gamal, *"Strong Functional Representation Lemma and Applications to Coding Theorems,"* IEEE Trans. Inf. Theory, 2018.

[9] Andrés, Bordenabe, Chatzikokolakis and Palamidessi, *"Geo-indistinguishability: Differential privacy for location-based systems,"* CCS 2013.

[10] Chen, Song, Ozgur and Kairouz, *"Privacy Amplification via Compression: Achieving the Optimal Privacy-Accuracy-Communication Trade-off in Distributed Mean Estimation,"* NeurIPS 2023.