Supplementary Material: Computing Tight Differential Privacy Guarantees Using FFT

A Proofs for the results of Section 3

A.1 Integral representation for exact DP-guarantees

Throughout this section we denote for neighbouring datasets X and Y the density function of $\mathcal{M}(X)$ with $f_X(t)$ and the density function of $\mathcal{M}(Y)$ with $f_Y(t)$.

Definition A.1. *A randomised algorithm $\mathcal{M}$ with an output of continuous one dimensional distributions satisfies (ε, δ)-DP if for every set $S \subset \mathbb{R}$ and every neighbouring datasets X and Y*

$$\int_S f_X(t) \, \mathrm{d}t \leq \mathrm{e}^{\varepsilon} \int_S f_Y(t) \, \mathrm{d}t + \delta \quad \text{and} \quad \int_S f_Y(t) \, \mathrm{d}t \leq \mathrm{e}^{\varepsilon} \int_S f_X(t) \, \mathrm{d}t + \delta.$$

We call $\mathcal{M}$ tightly (ε, δ)-DP, if there does not exist $\delta' < \delta$ such that $\mathcal{M}$ is (ε, δ')-DP.

The following auxiliary lemma is needed to obtain the representation given by Lemma A.4 (see [3, Lemma 1] for the discrete valued version of the result).

Lemma A.2. *$\mathcal{M}$ is tightly (ε, δ)-DP with*

$$\delta(\varepsilon) = \max_{X \sim Y} \left\{ \int_{\mathbb{R}} \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\} \, \mathrm{d}t, \int_{\mathbb{R}} \max\{f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t), 0\} \, \mathrm{d}t \right\}. \tag{A.1}$$

Proof. Assume $\mathcal{M}$ is tightly (ε, δ)-DP. Then, for every set $S \subset \mathbb{R}$ and every neighbouring datasets X and Y,

$$\begin{aligned} \int_S f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t) \, \mathrm{d}t &\leq \int_S \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\} \, \mathrm{d}t \\ &\leq \int_{\mathbb{R}} \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\} \, \mathrm{d}t. \end{aligned}$$

We get an analogous bound for $\int_S f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t)\, \mathrm{d}t$. By Definition A.1,

$$\delta \leq \max \left\{ \int\limits_{\mathbb{R}} \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\}\, \mathrm{d}t, \int\limits_{\mathbb{R}} \max\{f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t), 0\}\, \mathrm{d}t \right\}.$$

To show that the above inequality is tight, consider the set

$$S = \{t \in \mathbb{R} \,:\, f_X(t) \geq \mathrm{e}^{\varepsilon} f_Y(t)\}.$$

Then,

$$\begin{aligned} \int\limits_S f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t)\, \mathrm{d}t &= \int\limits_S \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\}\, \mathrm{d}t \\ &= \int\limits_{\mathbb{R}} \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\}\, \mathrm{d}t. \end{aligned} \tag{A.2}$$

Next, consider the set

$$S = \{t \in \mathbb{R} \,:\, f_Y(t) \geq \mathrm{e}^{\varepsilon} f_X(t)\}.$$

Similarly,

$$\int\limits_S f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t)\, \mathrm{d}t = \int\limits_{\mathbb{R}} \max\{f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t), 0\}\, \mathrm{d}t. \tag{A.3}$$

From (A.2) and (A.3) it follows that there exists a set $S \subset \mathbb{R}$ such that either

$$\int_S f_X(t)\, \mathrm{d}t = \mathrm{e}^{\varepsilon} \int_S f_Y(t)\, \mathrm{d}t + \delta \quad \text{or} \quad \int_S f_Y(t)\, \mathrm{d}t = \mathrm{e}^{\varepsilon} \int_S f_X(t)\, \mathrm{d}t + \delta$$

for δ given by (A.1). This shows that δ given by (A.1) is tight. □

The next lemma gives an integral representation for the right hand side of (A.1) involving the distribution function of the PLD (see also Lemma 5 of [5]). First we need the following definition.

Definition A.3. *Let $\mathcal{M} : \mathcal{X}^N \to \mathbb{R}$ be a randomised mechanism and let $X \sim Y$. Let $f_X(t)$ denote the density function of $\mathcal{M}(X)$ and $f_Y(t)$ the density function of $\mathcal{M}(Y)$. Assume $f_X(t) > 0$ and $f_Y(t) > 0$ for all $t \in \mathbb{R}$. We define the privacy loss function of f_X over f_Y as*

$$\mathcal{L}_{X/Y}(t) = \log \frac{f_X(t)}{f_Y(t)}.$$

Lemma A.4. *Let $\mathcal{M}$ be defined as above. $\mathcal{M}$ is tightly (ε, δ)-DP for*

$$\delta(\varepsilon) = \max_{X \sim Y} \max\{\delta_{X/Y}(\varepsilon), \delta_{Y/X}(\varepsilon)\},$$

where

$$\delta_{X/Y}(\varepsilon) = \int\limits_{\mathcal{L}_{X/Y}(\mathbb{R}) \cap [\varepsilon,\infty)} (1 - \mathrm{e}^{\varepsilon - s}) f_X\left(\mathcal{L}_{X/Y}^{-1}(s)\right) \frac{\mathrm{d}\mathcal{L}_{X/Y}^{-1}(s)}{\mathrm{d}s} \,\mathrm{d}s,$$

$$\delta_{Y/X}(\varepsilon) = \int\limits_{\mathcal{L}_{Y/X}(\mathbb{R}) \cap [\varepsilon,\infty)} (1 - \mathrm{e}^{\varepsilon - s}) f_Y\left(\mathcal{L}_{Y/X}^{-1}(s)\right) \frac{\mathrm{d}\mathcal{L}_{Y/X}^{-1}(s)}{\mathrm{d}s} \,\mathrm{d}s.$$

Proof. Consider the privacy loss function $\mathcal{L}_{X/Y}(t) = \log \frac{f_X(t)}{f_Y(t)}$. Denote $s = \mathcal{L}_{X/Y}(t)$. Then, it clearly holds $f_Y(t) = \mathrm{e}^{-s} f_X(t)$ and

$$\begin{aligned} \max\{f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t), 0\} &= \max\{0, (1 - \mathrm{e}^{\varepsilon - s}) f_X(t)\} \\ &= \begin{cases} (1 - \mathrm{e}^{\varepsilon - s}) f_X(t), & \text{if } s > \varepsilon, \\ 0, & \text{otherwise.} \end{cases} \end{aligned} \tag{A.4}$$

Consider next the integral $\int_{\mathbb{R}} \max\{0, f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t)\} \,\mathrm{d}t$. By making the change of variables $t = \mathcal{L}_{X/Y}^{-1}(s)$ and using (A.4), we see that

$$\begin{aligned} \int\limits_{\mathbb{R}} \max\{0, f_X(t) - \mathrm{e}^{\varepsilon} f_Y(t)\} \,\mathrm{d}t &= \int\limits_{\mathbb{R}} \max\{0, (1 - \mathrm{e}^{\varepsilon - s}) f_X(t)\} \,\mathrm{d}t \\ &= \int\limits_{\mathcal{L}_{X/Y}(\mathbb{R})} \max\left\{0,\ (1 - \mathrm{e}^{\varepsilon - s}) f_X\big(\mathcal{L}_{X/Y}^{-1}(s)\big) \frac{\mathrm{d}\mathcal{L}_{X/Y}^{-1}(s)}{\mathrm{d}s}\right\} \mathrm{d}s \\ &= \int\limits_{\mathcal{L}_{X/Y}(\mathbb{R}) \cap [\varepsilon,\infty)} (1 - \mathrm{e}^{\varepsilon - s}) f_X\big(\mathcal{L}_{X/Y}^{-1}(s)\big) \frac{\mathrm{d}\mathcal{L}_{X/Y}^{-1}(s)}{\mathrm{d}s} \,\mathrm{d}s, \end{aligned}$$

since $\frac{\mathrm{d}\mathcal{L}_{X/Y}^{-1}(s)}{\mathrm{d}s} \geq 0$ for all $s \in \mathcal{L}_{X/Y}(\mathbb{R})$. Analogously, we see that

$$\int\limits_{\mathbb{R}} \max\{0, f_Y(t) - \mathrm{e}^{\varepsilon} f_X(t)\} \,\mathrm{d}t = \int\limits_{\mathcal{L}_{Y/X}(\mathbb{R}) \cap [\varepsilon,\infty)} (1 - \mathrm{e}^{\varepsilon - s}) f_Y\big(\mathcal{L}_{Y/X}^{-1}(s)\big) \frac{\mathrm{d}\mathcal{L}_{Y/X}^{-1}(s)}{\mathrm{d}s} \,\mathrm{d}s.$$

The claim follows then from Lemma A.2. □

Definition A.5. *Let the assumptions of Definition A.3 of the main text hold and suppose* $\mathcal{L}_{X/Y} : \mathbb{R} \to D$*,* $D \subset \mathbb{R}$ *is a continuously differentiable bijective function. The privacy loss distribution (PLD) of* $\mathcal{M}(X)$ *over* $\mathcal{M}(Y)$ *is defined to be a random variable which has the density function*

$$\omega_{X/Y}(s) = \begin{cases} f_X\left(\mathcal{L}_{X/Y}^{-1}(s)\right) \frac{\mathrm{d}\mathcal{L}_{X/Y}^{-1}(s)}{\mathrm{d}s}, & s \in \mathcal{L}_{X/Y}(\mathbb{R}), \\ 0, & \textit{else.} \end{cases}$$

We directly get from Lemma A.4 the following representation.

Corollary A.6. *A randomised algorithm* $\mathcal{M}$ *with an output of continuous one dimensional distributions is tightly* (ε, δ)*-DP for*

$$\delta(\varepsilon) = \max_{X \sim Y} \max\{\delta_{X/Y}(\varepsilon), \delta_{Y/X}(\varepsilon)\}, \tag{A.5}$$

where

$$\delta_{X/Y}(\varepsilon) = \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s})\, \omega_{X/Y}(s)\, \mathrm{d}s, \quad \delta_{Y/X}(\varepsilon) = \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s})\, \omega_{Y/X}(s)\, \mathrm{d}s.$$

A.2 Privacy loss distribution of compositions

In order to use the representation given by Corollary A.6 for a composition of several mechanisms, we need to be able to evaluate the privacy loss distribution for compositions. This is given in the following theorem which is a continuous version of [5, Thm. 1].

Theorem A.7. *Let* X, Y *be adjacent datasets and let* $f_X(t)$ *denote the density function of* $\mathcal{M}(X)$*,* $f_Y(t)$ *that of* $\mathcal{M}(Y)$*,* $f_{X'}(t)$ *that of* $\mathcal{M}'(X)$ *and* $f_{Y'}(t)$ *that of* $\mathcal{M}'(Y)$*. Consider the PLD* $\omega^{\mathrm{c}}_{X/Y}$ *of the composition of* $\mathcal{M}$ *and* $\mathcal{M}'$ *(either* $\mathcal{M} \circ \mathcal{M}'$ *or* $\mathcal{M}' \circ \mathcal{M}$*). Denote by* $\omega_{X/Y}$ *the PLD of* $\mathcal{M}(X)$ *over* $\mathcal{M}(Y)$ *and by* $\omega_{X'/Y'}$ *the PLD of* $\mathcal{M}'(X)$ *over* $\mathcal{M}'(Y)$*. The density function of* $\omega^{\mathrm{c}}_{X/Y}$ *is given by*

$$\omega^{\mathrm{c}}_{X/Y}(s) = \int_{-\infty}^{\infty} \omega_{X/Y}(t) \omega_{X'/Y'}(s - t)\, \mathrm{d}t.$$

Proof. We first show that the privacy loss function of a composition is a sum of privacy loss functions. Let $\mathcal{L}^{c}_{X/Y}$ denote the privacy loss function of the composition mechanism. Then,

$$\begin{aligned} \mathcal{L}^{c}_{X/Y}(t_1, t_2) &= \log\left(\frac{f_{X,X'}(t_1, t_2)}{f_{Y,Y'}(t_1, t_2)}\right) = \log\left(\frac{f_X(t_1) f_{X'}(t_2)}{f_Y(t_1) f_{Y'}(t_2)}\right) \\ &= \log\left(\frac{f_X(t_1))}{f_Y(t_1))}\right) + \log\left(\frac{f_{X'}(t_2)}{f_{Y'}(t_2)}\right) \\ &= \mathcal{L}_{X/Y}(t_1) + \mathcal{L}_{X'/Y'}(t_2). \end{aligned} \tag{A.6}$$

Let $S \in \mathbb{R}$ be a measurable set. By using the property (A.6) and by change of variables we see that

$$\begin{aligned}
\omega^C_{X/Y}(S) &= \iint\limits_{\{(t_1,t_2)\in\mathbb{R}^2\,:\,\mathcal{L}_c(t_1,t_2)\in S\}} f_{X,X'}(t_1,t_2)\,\mathrm{d}t_1\,\mathrm{d}t_2 \\
&= \iint\limits_{\{(t_1,t_2)\in\mathbb{R}^2\,:\,\mathcal{L}_{X/Y}(t_1)+\mathcal{L}_{X'/Y'}(t_2)\in S\}} f_X(t_1)f_{X'}(t_2)\,\mathrm{d}t_1\,\mathrm{d}t_2 \\
&= \iint\limits_{\{s_1+s_2\in S\}\cap\{\mathcal{L}_{X/Y}(\mathbb{R})+\mathcal{L}_{X'/Y'}(\mathbb{R})\}} f_X\big(\mathcal{L}^{-1}_{X/Y}(s_1)\big)\,\frac{\mathrm{d}\mathcal{L}^{-1}_{X/Y}(s_1)}{\mathrm{d}s}\cdot \\
&\qquad f_{X'}\big(\mathcal{L}^{-1}_{X'/Y'}(s_2)\big)\,\frac{\mathrm{d}\mathcal{L}^{-1}_{X'/Y'}(s_2)}{\mathrm{d}s}\,\mathrm{d}s_1\,\mathrm{d}s_2 \\
&= \iint\limits_{\{s_1+s_2\in S\}} \omega_{X/Y}(s_1)\omega_{X'/Y'}(s_2)\,\mathrm{d}s_1\,\mathrm{d}s_2 \\
&= \int\limits_S \left(\int\limits_{-\infty}^{\infty} \omega_{X/Y}(s_1)\omega_{X'/Y'}(t-y_1)\,\mathrm{d}s_1\right)\,\mathrm{d}t.
\end{aligned}$$

□

From Corollary A.6 and Theorem A.7 we get the following integral formula for $\delta(\varepsilon)$.

Corollary A.8. *Consider k consecutive applications of a mechanism $\mathcal{M}$. Let $\varepsilon > 0$. The composition is tightly (ε,δ)-DP for δ given by*

$$\delta(\varepsilon) = \max_{X\sim Y} \max\{\delta_{X/Y}(\varepsilon), \delta_{Y/X}(\varepsilon)\},$$

where

$$\delta_{X/Y}(\varepsilon) = \int\limits_{\varepsilon}^{\infty} (1-\mathrm{e}^{\varepsilon-s})\left(\omega_{X/Y} *^k \omega_{X/Y}\right)(s)\,\mathrm{d}s,$$

where $(\omega_{X/Y} *^k \omega_{X/Y})(s)$ denotes the density function obtained by convolving $\omega_{X/Y}$ by itself k times (an analogous formula holds for $\delta_{Y/X}(\varepsilon)$).

We also give the following result for the relation between $\omega_{X/Y}$ and $\omega_{Y/X}$. This result can be used to determine which the value $\max\{\delta_{X/Y}, \delta_{Y/X}\}$. This result can be seen as a continuous version of Lemma 2 in [5].

Lemma A.9. *Let the privacy loss functions $\mathcal{L}_{X/Y}$ and $\mathcal{L}_{Y/X}$ and the privacy loss distributions $\omega_{X/Y}$ and $\omega_{Y/X}$. Then, it holds $\mathcal{L}_{Y/X}(\mathbb{R}) = \{\, t \in \mathbb{R} \;:\; -t \in \mathcal{L}_{X/Y}(\mathbb{R})\}$ and for all $y \in \mathcal{L}_{X/Y}(\mathbb{R})$:*

$$\omega_{X/Y}(s) = \mathrm{e}^s \omega_{Y/X}(-s).$$

Proof. From the definition it follows that

$$\mathcal{L}_{X/Y}(t) = -\mathcal{L}_{Y/X}(t),$$

and therefore also

$$\mathcal{L}^{-1}_{Y/X}(s) = \mathcal{L}^{-1}_{X/Y}(-s) \tag{A.7}$$

for all $y \in \mathcal{L}_{X/Y}(\mathbb{R})$. Let $y \in \mathcal{L}_{X/Y}(\mathbb{R})$. Then,

$$\begin{aligned} \omega_{X/Y}(s) &= f_X\left(\mathcal{L}^{-1}_{X/Y}(s)\right) \frac{\mathrm{d}\mathcal{L}^{-1}_{X/Y}(s)}{\mathrm{d}s} \\ &= f_X\left(\mathcal{L}^{-1}_{X/Y}(s)\right) \frac{1}{\mathcal{L}'_{X/Y}(\mathcal{L}^{-1}_{X/Y}(s))}. \end{aligned} \tag{A.8}$$

We notice that

$$\begin{aligned} \frac{f_X(t)}{\mathcal{L}'_{X/Y}(t)} &= \frac{f_X(t)}{\frac{f'_X(t)}{f_X(t)} - \frac{f'_Y(t)}{f_Y(t)}} \\ &= \frac{f_X(t)^2 f_Y(t)}{f'_X(t) f_Y(t) - f'_Y(t) f_X(t)} \\ &= \frac{f_X(t)}{f_Y(t)} \frac{f_X(t) f_Y(t)^2}{f'_X(t) f_Y(t) - f'_Y(t) f_X(t)} \\ &= \mathrm{e}^{\mathcal{L}_{X/Y}(t)} \frac{f_Y(t)}{\mathcal{L}'_{Y/X}(t)} \end{aligned}$$

and the claim follows using (A.8) and (A.7). □

One easily verifies the following corollary of Lemma A.9.

Corollary A.10. *For the convolutions it holds*

$$\left(\omega_{X/Y} *^k \omega_{X/Y}\right)(s) = \mathrm{e}^s \left(\omega_{Y/X} *^k \omega_{Y/X}\right)(-s).$$

B Tight privacy bounds for the Gaussian mechanism via one dimensional distributions

In this Section we show that the tight bounds of DP-SGD can be carried out by analysis of one dimensional mixture distributions. This equivalence has also been used in [1, Proof of Lemma 3]. We consider three different subsampling methods: sampling without replacement, sampling with replacement and Poisson subsampling (see [2] for further details).

In the next subsection we also rigorously show that tight privacy bounds for DP-SGD can be obtained from the analysis of one dimensional distributions.

B.1 Equivalence of the privacy bounds between the multidimensional and one dimensional mechanisms

As an example, we consider the Poisson subsampling. In this case each member of the dataset is included in the stochastic gradient minibatch with probability q. This means that each data element can appear at most once in the sample. The basic mechanism $\mathcal{M}$ is then of the form

$$\mathcal{M}(X) = \sum_{x \in B} f(x) + \mathcal{N}(0, \sigma^2 I_d),$$

where B is a randomly drawn subset of $\{x_1, \ldots, x_N\}$ and $\|f(x)\|_2 \leq 1$ for all $x \in B$.

Consider the case of remove/add relation $\sim_R$ and let X and Y be neighbouring datasets. Consider first the case $q = 1$, i.e., $|B| = N$. The condition of (ε, δ)-differential privacy states that for every measurable set $S \subset \mathbb{R}^d$ and every neighbouring X and Y:

$$\mathbb{P}(\mathcal{M}(X) \in S) \leq \mathrm{e}^{\varepsilon} \mathbb{P}(\mathcal{M}(Y) \in S) + \delta. \tag{B.1}$$

Suppose $X = Y \cup \{x'\}$ and assume $\|f(x')\|_2 = 1$. and we easily see that this is then equivalent to the condition that for every measurable set $S \subset \mathbb{R}^d$:

$$\mathbb{P}\big(\mathcal{N}(f(x)', \sigma^2 I_d) \in S\big) \leq \mathrm{e}^{\varepsilon} \mathbb{P}\big(\mathcal{N}(0, \sigma^2 I_d) \in S\big) + \delta. \tag{B.2}$$

Let $U \in \mathbb{R}^{d \times d}$ be a unitary matrix such that

$$U f(x') = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} =: e_1.$$

This means that U is of the form $U = \begin{bmatrix} f(x') & \widetilde{U} \end{bmatrix}$, where $\widetilde{U}$ can be taken as any $d \times (d-1)$ matrix with orthonormal columns such that $\widetilde{U}^T f(x') = 0$.

Due to the unitarity of U, the condition (B.2) is equivalent to the condition that for every measurable set $S \subset \mathbb{R}^d$:

$$\mathbb{P}\big(U\mathcal{N}(f(x'),\sigma^2 I_d) \in US\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(U\mathcal{N}(0,\sigma^2 I_d) \in US\big) + \delta. \tag{B.3}$$

Furthermore, due to the unitarity of U, $U\mathcal{N}(0,\sigma^2 I_d) \sim \mathcal{N}(0,\sigma^2 I_d)$ and we see that (B.3) is equivalent to the condition that for every measurable set $S \subset \mathbb{R}^d$:

$$\mathbb{P}\big(\mathcal{N}(e_1,\sigma^2 I_d) \in US\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(\mathcal{N}(0,\sigma^2 I_d) \in US\big) + \delta, \tag{B.4}$$

where $US = \{Ux \,:\, x \in S\}$. Then, we see that the condition (B.3) is equivalent to the condition that for every measurable set $S \subset \mathbb{R}$:

$$\mathbb{P}\big(\mathcal{N}(1,\sigma^2) \in S\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(\mathcal{N}(0,\sigma^2) \in S\big) + \delta. \tag{B.5}$$

Thus, if X and Y are given as above, finding the parameters ε and δ that satisfy (B.1) amounts to finding values of ε and δ that satisfy (B.5).

When $q < 1$, we see that $f(x')$ is in B with a probability q. Reasoning as above, we arrive at the the condition that for every measurable set $S \subset \mathbb{R}^d$:

$$\mathbb{P}\big(\, q\,\mathcal{N}(f(x'),\sigma^2 I_d) + (1-q)\,\mathcal{N}(0,\sigma^2 I_d) \in S\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(\mathcal{N}(0,\sigma^2 I_d) \in S\big) + \delta,$$

where $q\mathcal{N}(f(x'),\sigma^2 I_d) + (1-q)\mathcal{N}(0,\sigma^2 I_d)$ denotes a mixture distribution. Similarly, this leads to considering the one dimensional neighbouring distributions

$$f_X := q\mathcal{N}(1,\sigma^2) + (1-q)\mathcal{N}(0,\sigma^2) \quad \text{and} \quad f_Y := \mathcal{N}(0,\sigma^2).$$

In order the condition (B.1) holds for all $X \sim_R Y$, then it has to hold that for every measurable set $S \subset \mathbb{R}$ both

$$\mathbb{P}\big(f_X \in S\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(f_Y \in S\big) + \delta \quad \text{and} \quad \mathbb{P}\big(f_Y \in S\big) \leq \mathrm{e}^{\varepsilon}\mathbb{P}\big(f_X \in S\big) + \delta.$$

With an analogous reasoning, we see that in the case of substitution relation $\sim_S$ the worst case is obtained by considering the neighbouring distributions

$$q\mathcal{N}(1,\sigma^2) + (1-q)\mathcal{N}(0,\sigma^2)$$

and

$$q\mathcal{N}(-1,\sigma^2) + (1-q)\mathcal{N}(0,\sigma^2).$$

Finally, we note that the case $\|f(x')\|_2 < 1$ would lead to neighbouring distributions f_X and f_Y that are closer to each other than in the case $\|f(x')\|_2 = 1$. This would give tighter (ε,δ)-values, i.e., $\|f(x')\|_2 = 1$ gives the worst case. This could be shown rigorously by scaling the parameter σ and considering the analysis below.

B.2 Poisson subsampling

B.2.1 Neighbouring relation with remove/add

As shown above, for the analysis in case of Poisson subsampling it is sufficient to consider the density functions (see also [8] and [3])

$$\begin{aligned} f_X(t) &= q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}, \\ f_Y(t) &= \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}. \end{aligned} \tag{B.6}$$

The privacy loss function $\mathcal{L}_{X/Y}(t)$ is then given by

$$\mathcal{L}_{X/Y}(t) = \log \frac{q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}}{\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}} = \log\left(q\,\mathrm{e}^{\frac{2t-1}{2\sigma^2}} + (1-q)\right).$$

We see that $\mathcal{L}_{X/Y}(\mathbb{R}) = (\log(1-q), \infty)$ and that $\mathcal{L}_{X/Y}$ is a strictly increasing continuously differentiable function in the whole $\mathbb{R}$. Straightforward calculation shows that

$$\mathcal{L}_{X/Y}^{-1}(s) = \sigma^2 \log \frac{\mathrm{e}^s - (1-q)}{q} + \frac{1}{2}$$

and

$$\frac{\mathrm{d}}{\mathrm{d}\,s}\mathcal{L}_{X/Y}^{-1}(s) = \frac{\sigma^2 \mathrm{e}^s}{\mathrm{e}^s - (1-q)}.$$

The privacy loss distribution $\omega_{X/Y}$ is then given by the density function

$$\frac{\mathrm{d}\,\omega_{X/Y}}{\mathrm{d}\,s}(s) = \begin{cases} f_X(\mathcal{L}_{X/Y}^{-1}(s))\frac{\mathrm{d}}{\mathrm{d}\,s}\mathcal{L}_{X/Y}^{-1}(s), & \text{if } s > \log(1-q), \\ 0, & \text{else.} \end{cases}$$

The privacy loss distribution $\frac{\mathrm{d}\omega_{X/Y}}{\mathrm{d}s}$ has its mass mostly on the positive real axis (equals zero for $y \leq \log(1-q)$) and so do the the convolutions $\frac{\mathrm{d}\omega_{X/Y}}{\mathrm{d}s} *^k \frac{\mathrm{d}\omega_{X/Y}}{\mathrm{d}s}$. Therefore, by Lemma A.9 and its corollary, we see that $\frac{\mathrm{d}\omega_{Y/X}}{\mathrm{d}s}$ has its mass mostly on the negative real axis (equals zero for $y \geq |\log(1-q)|$). Thus the representation (A.5) supports the numerical observation that generally $\delta = \delta_{X/Y}$.

B.3 Sampling without replacement and $\sim_S$-neighouring relation

Denote by m the batch size (fixed) and $q = m/N$. In case of sampling without replacement and $(\varepsilon, \delta, \sim_S)$-DP, the differing element is in the minibatch with a probability q, and without loss of generality, we may again consider the density functions

$$\begin{aligned} f_X(t) &= q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}, \\ f_Y(t) &= q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t+1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}. \end{aligned} \tag{B.7}$$

The privacy loss function is then given by

$$\mathcal{L}_{X/Y}(t) = \log\left(\frac{q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}}{q\,\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t+1)^2}{2\sigma^2}} + (1-q)\frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}}\right) = \log\left(\frac{q\,\mathrm{e}^{\frac{2t-1}{2\sigma^2}} + (1-q)}{q\,\mathrm{e}^{\frac{-2t-1}{2\sigma^2}} + (1-q)}\right).$$

Now $\mathcal{L}_{X/Y}(\mathbb{R}) = \mathbb{R}$ and $\mathcal{L}_{X/Y}$ is again a strictly increasing continuously differentiable function in the whole $\mathbb{R}$. Denote

$$x = \mathrm{e}^{\frac{t}{\sigma^2}} \quad \text{and} \quad c = q\mathrm{e}^{-\frac{1}{2\sigma^2}}.$$

Then, solving $\mathcal{L}_{X/Y}(t) = s$ leads to the equation

$$\begin{aligned} & \frac{cx + (1-q)}{cx^{-1} + (1-q)} = \mathrm{e}^s \\ \iff\quad & cx^2 + (1-q)(1-\mathrm{e}^s)x - c\mathrm{e}^s = 0 \\ \overset{x>0}{\iff}\quad & x = \frac{-(1-q)(1-\mathrm{e}^s) + \sqrt{(1-q)^2(1-\mathrm{e}^s)^2 + 4c^2\mathrm{e}^s}}{2c}. \end{aligned}$$

We find that

$$\mathcal{L}_{X/Y}^{-1}(s) = \sigma^2 \log\left(\frac{-(1-q)(1-\mathrm{e}^s) + \sqrt{(1-q)^2(1-\mathrm{e}^s)^2 + 4c^2\mathrm{e}^s}}{2c}\right)$$

and

$$\frac{\mathrm{d}}{\mathrm{d}\,s}\mathcal{L}_{X/Y}^{-1}(s) = \sigma^2 \frac{\frac{4c^2\mathrm{e}^s - 2(1-q)^2\mathrm{e}^s(1-\mathrm{e}^s)}{2\sqrt{4c^2\mathrm{e}^s + (1-q)^2(1-\mathrm{e}^s)^2}} + (1-q)\mathrm{e}^s}{\sqrt{4c^2\mathrm{e}^s + (1-q)^2(1-\mathrm{e}^s)^2} - (1-q)(1-\mathrm{e}^s)}.$$

In case of odd loss functions ($f_Y(-t) = f_X(t)$ and $\mathcal{L}_{X/Y}(-t) = -\mathcal{L}_{X/Y}(t)$) we have the following:

$$\frac{\mathrm{d}\omega_{X/Y}}{\mathrm{d}s}(s) = \frac{\mathrm{d}\omega_{Y/X}}{\mathrm{d}s}(s).$$

This follows from using the oddity of $\mathcal{L}_{X/Y}$ and Lemma A.9. Therefore, if $f_Y(-t) = f_X(t)$ and $\mathcal{L}_{X/Y}(-t) = -\mathcal{L}_{X/Y}(t)$, it holds $\delta = \delta_{Y/X} = \delta_{X/Y}$ by the representation (A.5).

We remark that in $(\varepsilon, \delta, \sim_S)$-DP, the Poisson subsampling with the sampling parameter γ (i.e., each sample is in the batch with a probability γ) is equivalent to the case of the sampling with replacement with $q = \gamma$, as in both cases the differing element is included in the minibatch with probability γ.

B.4 Sampling with replacement and $\sim_S$-neighouring relation

Consider next the sampling with replacement and the $\sim_S$-neighbouring relation. Then the number of times the differing sample x' is in the batch is binomially distributed, i.e., the probability for being in the batch ℓ times is $\left(\frac{1}{n}\right)^{\ell}\left(\frac{1}{n}\right)^{m-\ell}\binom{m}{\ell}$, where m denotes the batch size and n the total number of data samples.

Then, without loss of generality, we may consider the density functions (m denotes the batch size)

$$
\begin{aligned}
f_X(t) &= \frac{1}{\sqrt{2\pi\sigma^2}} \sum_{\ell=0}^{m} q^{\ell}(1-q)^{m-\ell}\binom{m}{\ell}\, \mathrm{e}^{\frac{-(t-\ell)^2}{2\sigma^2}}, \\
f_Y(t) &= \frac{1}{\sqrt{2\pi\sigma^2}} \sum_{\ell=0}^{m} q^{\ell}(1-q)^{m-\ell}\binom{m}{\ell}\, \mathrm{e}^{\frac{-(t+\ell)^2}{2\sigma^2}},
\end{aligned}
\tag{B.8}
$$

where $q = 1/n$. The privacy loss function is then given by

$$
\mathcal{L}_{X/Y}(t) = \log\left(\frac{\sum\limits_{\ell=0}^{m} q^{\ell}(1-q)^{m-\ell}\binom{m}{\ell}\,\mathrm{e}^{\frac{-(t-\ell)^2}{2\sigma^2}}}{\sum\limits_{\ell=0}^{m} q^{\ell}(1-q)^{m-\ell}\binom{m}{\ell}\,\mathrm{e}^{\frac{-(t+\ell)^2}{2\sigma^2}}}\right) = \log\left(\frac{\sum\limits_{\ell=0}^{m} c_\ell x^{\ell}}{\sum\limits_{\ell=0}^{m} c_\ell x^{-\ell}}\right),
$$

where

$$
c_\ell = q^{\ell}(1-q)^{m-\ell}\binom{m}{\ell}\,\mathrm{e}^{\frac{-\ell^2}{2\sigma^2}} \quad \text{and} \quad x = \mathrm{e}^{\frac{t}{\sigma^2}}. \tag{B.9}
$$

Since $c_\ell > 0$ for all $\ell = 1, \ldots, m$, clearly $\sum_{\ell=0}^{m} c_\ell x^{\ell}$ is strictly increasing as a function of t and $\sum_{\ell=0}^{m} c_\ell x^{-\ell}$ is strictly decreasing. Moreover, we see that

$$
\frac{\sum_{\ell=0}^{m} c_\ell x^{\ell}}{\sum_{\ell=0}^{m} c_\ell x^{-\ell}} \to 0 \quad \text{as } t \to -\infty \qquad \text{and} \qquad \frac{\sum_{\ell=0}^{m} c_\ell x^{\ell}}{\sum_{\ell=0}^{m} c_\ell x^{-\ell}} \to \infty \quad \text{as } t \to \infty.
$$

Thus, $\mathcal{L}_{X/Y}(\mathbb{R}) = \mathbb{R}$ and $\mathcal{L}_{X/Y}(t)$ is a strictly increasing continuously differentiable function in the whole $\mathbb{R}$. To find $\mathcal{L}_{X/Y}^{-1}(s)$ one needs to solve $\mathcal{L}_{X/Y}(t) = s$, i.e., one needs to find the single real root of a polynomial of order $2m$.

To find $\mathcal{L}_{X/Y}^{-1}(s)$, i.e. to solve $\mathcal{L}_{X/Y}(t) = s$ for a given y, one may use e.g. Newton's method.

C Error estimates

For the error analysis we consider the Poisson subsampling with $(\varepsilon, \delta, \sim_R)$-DP, i.e., we consider the PLD density function (Sec. B.2.1)

$$\omega(s) = \begin{cases} f(g(s))g'(s), & \text{if } s > \log(1-q), \\ 0, & \text{otherwise,} \end{cases} \tag{C.1}$$

where

$$\begin{aligned} f(t) &= \frac{1}{\sqrt{2\pi\sigma^2}} [q \mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\mathrm{e}^{-\frac{t^2}{2\sigma^2}}], \\ g(s) &= \sigma^2 \log\left(\frac{\mathrm{e}^s - (1-q)}{q}\right) + \frac{1}{2}. \end{aligned}$$

Theorem C.1. *Let the vector C^k be defined as in Sec. 5.3. Total error of the approximation (determined by the truncation parameter L and the discretisation parameter n) can be bounded by three terms as follows:*

$$\left| \int_\varepsilon^\infty (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k \right| \leq I_1(L) + I_2(L) + I_3(L, n),$$

where

$$\begin{aligned} I_1(L) &= \left| \int_L^\infty (\omega *^k \omega)(s) \, \mathrm{d}s \right|, \\ I_2(L) &= \left| \int_\varepsilon^L (\omega *^k \omega)(s) - (\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s \right|, \\ I_3(L, n) &= \left| \int_\varepsilon^L (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k \right|. \end{aligned}$$

Proof. By adding and subtracting terms and using the triangle inequality, we get

$$
\begin{aligned}
&\left| \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k \right| \\
\leq &\left| \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s - \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s \right| \\
&\quad + \left| \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s - \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s \right| \\
&\quad + \left| \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k \right| \\
\leq &\left| \int_{L}^{\infty} (\omega *^k \omega)(s) \, \mathrm{d}s \right| + \left| \int_{\varepsilon}^{L} (\omega *^k \omega)(s) - (\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s \right| \\
&\quad + \left| \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s) \, \mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k \right| .
\end{aligned} \tag{C.2}
$$

□

We consider next separately each of the three terms on the right hand side of (C.2).

C.1 Tail bounds for the convolved PLDs

The first term on the right hand side of (C.2) is bounded by the tail of the convolved PLDs:

$$
\left| \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s - \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s) \, \mathrm{d}s \right| \leq \int_{L}^{\infty} (\omega *^k \omega)(s) \, \mathrm{d}s. \tag{C.3}
$$

In this Section we show how to use existing Rényi differential privacy (RDP) results to bound the tail (C.3).

The Chernoff bound (see e.g. [7]) states that for any random variable X and for all $\lambda > 0$ it holds

$$
\mathbb{P}[X \geq t] = \mathbb{P}[\mathrm{e}^{\lambda X} \geq \mathrm{e}^{\lambda t}] \leq \frac{\mathbb{E}[\mathrm{e}^{\lambda X}]}{\mathrm{e}^{\lambda t}}. \tag{C.4}
$$

From the RDP bounds given in [4] we obtain the following bound for the moment generating function $\mathbb{E}[\mathrm{e}^{\lambda \omega}]$.

Lemma C.2. *Suppose* $q \leq \frac{1}{5}$ *and* $\sigma \geq 4$. *Suppose* λ *satisfies*

$$\begin{aligned} 1 <& \lambda \leq \frac{1}{2}\sigma^2 c - 2\log\sigma, \\ & \lambda \leq \frac{\frac{1}{2}\sigma^2 c - \log 5 - 2\log\sigma}{c + \log(q\lambda) + 1/(2\sigma^2)}, \end{aligned}$$

where $c = \log\left(1 + \frac{1}{q(\lambda-1)}\right)$. *Then,*

$$\mathbb{E}[\mathrm{e}^{\lambda\omega}] \leq 1 + \frac{2q^2(\lambda+1)\lambda}{\sigma^2}.$$

Proof. Making change of variables $y = \mathcal{L}(t)$ (recall: $\mathcal{L}(\mathbb{R}) = (\log(1-q), \infty)$ and $\mathcal{L}(t)$ is a strictly increasing differentiable function), we see a connection to the Rényi differential privacy:

$$\begin{aligned} \mathbb{E}[\mathrm{e}^{\lambda\omega}] &= \int_{\log(1-q)}^{\infty} \mathrm{e}^{\lambda s}\omega(s)\,\mathrm{d}s \\ &= \int_{-\infty}^{\infty} \mathrm{e}^{\lambda\mathcal{L}(t)} f_X(t)\,\mathrm{d}t \\ &= \int_{-\infty}^{\infty} \left(\frac{f_X(t)}{f_Y(t)}\right)^{\lambda} f_X(t)\,\mathrm{d}t \\ &= \int_{-\infty}^{\infty} \left(\frac{f_X(t)}{f_Y(t)}\right)^{\lambda+1} f_Y(t)\,\mathrm{d}t. \end{aligned}$$

Here $f_X(t) = q\mu_1(t) + (1-q)\mu_0(t)$, where $\mu_0(t) = \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}$ and $\mu_1(t) = \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}}$, and $f_Y(t) = \mu_0(t)$. Therefore

$$\mathbb{E}[\mathrm{e}^{\lambda\omega}] = \int_{-\infty}^{\infty} \left(\frac{f_X(t)}{f_Y(t)}\right)^{\lambda+1} f_Y(t)\,\mathrm{d}t = \int_{-\infty}^{\infty} \left((1-q) + q\frac{\mu_1(t)}{\mu_0(t)}\right)^{\lambda+1} \mu_0(t)\,\mathrm{d}t. \tag{C.5}$$

From the proof of [4, Thm. 11] we get a bound for (C.5) which shows the claim. □

Theorem C.3. *Let the assumptions on* σ *and* q *of Lemma C.2 hold. Assume* ω_i, $i = 1, \ldots, k$ *are independent PLDs of the form* (C.1) *determined by* σ *and* q. *Denote* $S_k := \sum_{i=1}^{k} \omega_i$. *Then, it holds*

$$\mathbb{P}(S_k \geq L) \leq \left(1 + \frac{2q^2(\lambda+1)\lambda}{\sigma^2}\right)^k \mathrm{e}^{-L\lambda}$$

for all λ *that satisfy the assumptions of Lemma C.2.*

Proof. Since ω_i's are independent, we have by Lemma C.2,

$$\mathbb{E}[\mathrm{e}^{\lambda S_k}] = \prod_{i=1}^{k} \mathbb{E}[\mathrm{e}^{\lambda \omega_i}] \leq \left(1 + \frac{2q^2(\lambda+1)\lambda}{\sigma^2}\right)^k.$$

Using the Chernoff bound, we find that

$$\mathbb{P}(S_k \geq L) \leq \left(1 + \frac{2q^2(\lambda+1)\lambda}{\sigma^2}\right)^k \mathrm{e}^{-L\lambda}$$

For all λ that satisfy the assumptions of Lemma C.2. □

The parameter λ in Theorem C.3 can be chosen freely as long as it satisfies the conditions of Lemma C.2. The λ that minimises the function $\lambda^2 \mathrm{e}^{-L\lambda}$ is given by $\lambda = \frac{L}{2}$. This choice leads to the following bound.

Corollary C.4. *Let L be chosen such that $\lambda = L/2$ satisfies the assumptions of Lemma C.2. Then, we have the following bound:*

$$\mathbb{P}(S_k \geq L) \leq \left(1 + \frac{2q^2(\frac{L}{2}+1)\frac{L}{2}}{\sigma^2}\right)^k \mathrm{e}^{-\frac{L^2}{2}}.$$

Notice that

$$\mathbb{P}(S_k \geq L) = \int_L^\infty (\omega *^k \omega)(s)\,\mathrm{d}s.$$

Example 1. Set $q = 0.01$, $\sigma = 4.0$. We numerically observe that the conditions of Lemma 9 hold up to $\lambda \approx 14.3$. Thus, Corollary 4 holds up to $L \approx 28.6$. Figure 1 shows the convergence of the bound with respect to L.

Example 2 (Illustration of the bound (7.3) of the main article). When $q = 0.01$ and $\sigma = 2.0$, the conditions of Lemma 9 of the main article hold for λ up to ≈ 9.5 (i.e. (7.3) holds for L up to ≈ 19). Figure 2 shows the convergence of the bound (7.3) in this case.

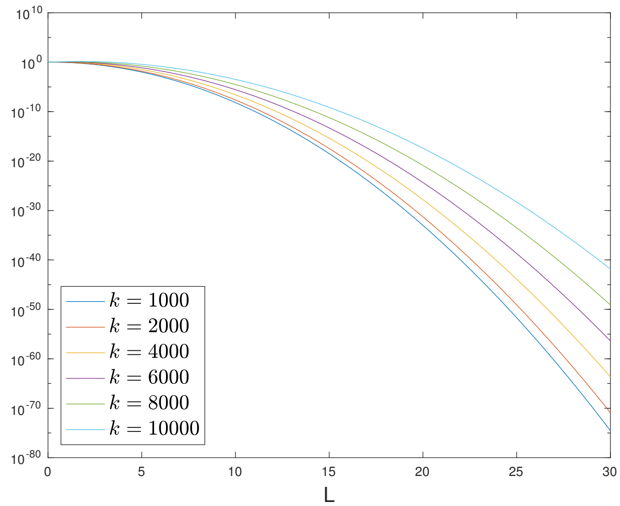

Figure 1: Convergence of the bound given by Corollary 4 for $q = 0.01$ and $\sigma = 4.0$.

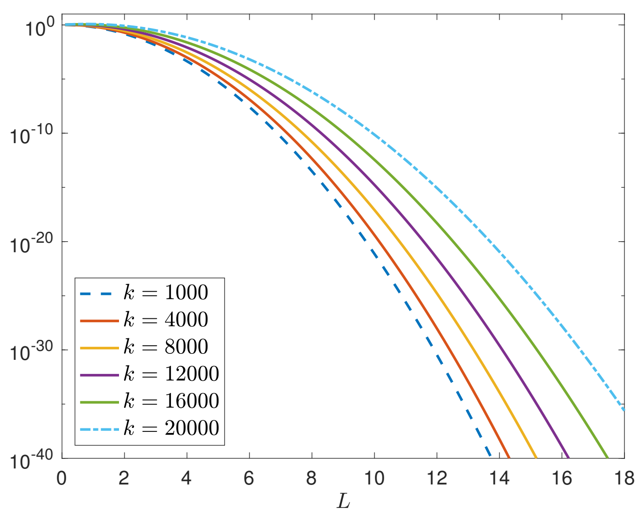

Figure 2: Convergence of the bound (7.3) of the main article for $q = 0.01$ and $\sigma = 2.0$ for different number of compositions k.

C.2 Errors arising from truncation of the convolution integrals and periodisation

We next bound the second term on the right hand side of (C.2), i.e. the term

$$\left| \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s)\, \mathrm{d}s - \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s)\, \mathrm{d}s \right|.$$

We easily see that this can be bounded as

$$\begin{aligned} &\left| \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\omega *^k \omega)(s)\, \mathrm{d}s - \int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s)\, \mathrm{d}s \right| \\ &\leq \int_{\varepsilon}^{L} \left| (\omega *^k \omega - \omega \circledast^k \omega)(x) \right| \, \mathrm{d}x + \int_{\varepsilon}^{L} \left| (\omega \circledast^k \omega - \widetilde{\omega} \circledast^k \widetilde{\omega})(x) \right| \, \mathrm{d}x \end{aligned} \tag{C.6}$$

C.2.1 Truncation of the convolution integrals

We first bound $\omega *^k \omega - \omega \circledast^k \omega$. We have the following pointwise bound.

Lemma C.5. *Let $\sigma > 0$ and $0 < q < \frac{1}{2}$. Let ω be defined as above, and let $L \geq 1$. Then, for all $x \in \mathbb{R}$,*

$$\left| (\omega *^k \omega - \omega \circledast^k \omega)(x) \right| \leq k\sigma \mathrm{e}^{-\frac{-(\sigma^2 L + C)^2}{2\sigma^2}},$$

where $C = \sigma^2 \log(\frac{1}{2q}) - \frac{1}{2}$

Proof. By adding and subtracting, we may write

$$\omega *^k \omega - \omega \circledast^k \omega = \omega \circledast (\omega *^{k-1} \omega - \omega \circledast^{k-1} \omega) + \omega \circledast (\omega \circledast^{k-1} \omega) - \omega * (\omega \circledast^{k-1} \omega), \tag{C.7}$$

where

$$\begin{aligned} &\omega \circledast (\omega \circledast^{k-1} \omega) - \omega * (\omega \circledast^{k-1} \omega)(x) \\ &= \int_{-L}^{L} \omega(t)(\omega \circledast^{k-1} \omega)(x - t)\, \mathrm{d}t - \int_{-\infty}^{\infty} \omega(t)(\omega \circledast^{k-1} \omega)(x - t)\, \mathrm{d}t \\ &= - \int_{L}^{\infty} \omega(t)(\omega \circledast^{k-1} \omega)(x - t)\, \mathrm{d}t, \end{aligned}$$

since $\omega(s) = 0$ for all $s < \log(1-q)$ and $-L < \log(1-q)$. Using Lemma D.3 of Appendix, we see that for all x,

$$\begin{aligned} \Big| \big(\omega \circledast (\omega \circledast^{k-1} \omega) - \omega * (\omega \circledast^{k-1} \omega) \big)(x) \Big| &\leq \max_{s \geq L} \omega(s) \int_L^\infty (\omega \circledast^{k-1} \omega)(x-t) \, \mathrm{d}t \\ &\leq \max_{s \geq L} \omega(s) \\ &\leq \sigma \mathrm{e}^{-\frac{-(\sigma^2 L + C)^2}{2\sigma^2}}. \end{aligned} \tag{C.8}$$

Using again Lemma D.3, we see that for all x,

$$\begin{aligned} |(\omega * \omega - \omega \circledast \omega)(x)| &= \int_{-\infty}^{\infty} \omega(t)\omega(x-t) \, \mathrm{d}t - \int_{-L}^{L} \omega(t)\omega(x-t) \, \mathrm{d}t \\ &= \int_L^\infty \omega(t)\omega(x-t) \, \mathrm{d}t \\ &\leq \max_{s \geq L} \omega(s) \int_L^\infty \omega(x-t) \, \mathrm{d}t \\ &\leq \sigma \mathrm{e}^{-\frac{-(\sigma^2 L + C)^2}{2\sigma^2}}. \end{aligned} \tag{C.9}$$

The claim follows from the recursion (C.7) and the bounds (C.8) and (C.9). □

C.2.2 Error arising from the periodisation

We next bound the second term on the right hand side of (C.6). The bound is expressed in terms of the the log of the moment generating function of the privacy loss function $\mathcal{L} = \mathcal{L}_{X/Y}$ (see also [1]) which is defined for all $\lambda > 0$ as

$$\alpha(\lambda) := \log \mathop{\mathbb{E}}_{t \sim f_X(t)} [\mathrm{e}^{\lambda \mathcal{L}(t)}].$$

As shown in equation (7.2) of the main text, $\alpha(\lambda)$ is related to the moment generating function of the privacy loss distribution as

$$\mathbb{E}[\mathrm{e}^{\lambda \omega}] = \mathrm{e}^{\alpha(\lambda)}. \tag{C.10}$$

Thus, using the Chernoff bound and (C.10), tail bounds involving ω can bounded in terms of $\alpha(\lambda)$. Bounds for $\alpha(\lambda)$ in the case of Poisson subsampling with $\sim_R$ neighbouring relation are given in [1] and [4].

Lemma C.6. *Let ω be defined as above. Then,*

$$\int_{\varepsilon}^{L} \left|(\omega \circledast^k \omega - \widetilde{\omega} \circledast^k \widetilde{\omega})(x)\right| \,\mathrm{d}x \le \mathrm{e}^{\alpha(L/2)}\mathrm{e}^{-\frac{L^2}{2}} + 2\sum_{n=1}^{\infty} \mathrm{e}^{k\alpha(nL)}\mathrm{e}^{-2(nL)^2}.$$

Proof. We see that

$$\begin{aligned}
&(\widetilde{\omega} \circledast^k \widetilde{\omega} - \omega \circledast^k \omega)(x) \\
&\quad= \int_{-L}^{L} \widetilde{\omega}(t_1)\dots\int_{-L}^{L} \widetilde{\omega}(t_{k-1})\,\widetilde{\omega}(x - \textstyle\sum_{i=1}^{k-1} t_i)\,\mathrm{d}t_1\dots\mathrm{d}t_{k-1} \\
&\qquad - \int_{-L}^{L} \omega(t_1)\dots\int_{-L}^{L} \omega(t_{k-1})\,\omega(x - \textstyle\sum_{i=1}^{k-1} t_i)\,\mathrm{d}t_1\dots\mathrm{d}t_{k-1} \\
&\quad= \int_{-L}^{L} \omega(t_1)\dots\int_{-L}^{L} \omega(t_{k-1})\,\widetilde{\omega}(x - \textstyle\sum_{i=1}^{k-1} t_i)\,\mathrm{d}t_1\dots\mathrm{d}t_{k-1} \\
&\qquad - \int_{-L}^{L} \omega(t_1)\dots\int_{-L}^{L} \omega(t_{k-1})\,\omega(x - \textstyle\sum_{i=1}^{k-1} t_i)\,\mathrm{d}t_1\dots\mathrm{d}t_{k-1} \\
&\quad= \int_{-L}^{L} \omega(t_1)\dots\int_{-L}^{L} \omega(t_{k-1})\Big(\widetilde{\omega}(x - \textstyle\sum_{i=1}^{k-1} t_i) - \omega(x - \textstyle\sum_{i=1}^{k-1} t_i)\Big)\,\mathrm{d}t_1\dots\mathrm{d}t_{k-1}
\end{aligned} \tag{C.11}$$

since $\omega = \widetilde{\omega}$ on the interval $[-L, L]$.

Recall that $\widetilde{\omega}$ is the $2L$-periodic function for which $\widetilde{\omega}(t) = \omega(t)$ for all $t \in [-L, L]$. Therefore

$$\widetilde{\omega}(t) - \omega(t) = \sum_{n\in\mathbb{Z}\setminus\{0\}} \widehat{\omega}_n(t) - r(t), \tag{C.12}$$

where

$$\widehat{\omega}_n(t) = \begin{cases} \omega(t - 2nL), & \text{if } t \in [(2n-1)L, (2n+1)L] \\ 0, & \text{else,} \end{cases}$$

and

$$r(t) = \begin{cases} \omega(t), & \text{if } t \ge L \\ 0, & \text{else.} \end{cases}$$

Thus, from (C.11) and (C.12) it follows that

$$(\widetilde{\omega} \circledast^k \widetilde{\omega} - \omega \circledast^k \omega)(x) = C_1(x) + C_2(x), \tag{C.13}$$

where

$$C_1(x) = \int_{-L}^{L} \omega(t_1) \dots \int_{-L}^{L} \omega(t_{k-1}) \sum_{n \in \mathbb{Z} \setminus \{0\}} \widehat{\omega}_n(x - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1}$$

and

$$C_2(x) = \int_{-L}^{L} \omega(t_1) \dots \int_{-L}^{L} \omega(t_{k-1}) r(x - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1}.$$

We see that $|C_1(x)|$ can be bounded as

$$\begin{aligned}
|C_1(x)| &= \int_{-L}^{L} \omega(t_1) \dots \int_{-L}^{L} \omega(t_{k-1}) \sum_{n \in \mathbb{Z} \setminus \{0\}} \widehat{\omega}_n(x - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1} \\
&= \sum_{n \in \mathbb{Z} \setminus \{0\}} \int_{-L}^{L} \omega(t_1) \dots \int_{-L}^{L} \omega(t_{k-1}) \, \widehat{\omega}_n(x - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1} \\
&\leq \sum_{n \in \mathbb{Z} \setminus \{0\}} \int_{-L}^{L} \omega(t_1) \dots \int_{-L}^{L} \omega(t_{k-1}) \, \omega(x - 2nL - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1} \\
&\leq \sum_{n \in \mathbb{Z} \setminus \{0\}} \int_{-\infty}^{\infty} \omega(t_1) \dots \int_{-\infty}^{\infty} \omega(t_{k-1}) \, \omega(x - 2nL - \textstyle\sum_{i=1}^{k-1} t_i) \, \mathrm{d}t_1 \dots \mathrm{d}t_{k-1} \\
&= \sum_{n \in \mathbb{Z} \setminus \{0\}} (\omega *^k \omega)(x - 2nL).
\end{aligned}$$

Next, consider the expression

$$\int_{\varepsilon}^{L} \sum_{n \in \mathbb{Z} \setminus \{0\}} (\omega *^k \omega)(x - 2nL) \, \mathrm{d}x = \sum_{n=1}^{\infty} \int_{\varepsilon}^{L} (\omega *^k \omega)(x - 2nL) \, \mathrm{d}x + \sum_{n=1}^{\infty} \int_{\varepsilon}^{L} (\omega *^k \omega)(x + 2nL) \, \mathrm{d}x. \quad \text{(C.14)}$$

Clearly, for the second term on the right hand side of (C.14),

$$\begin{aligned}
\sum_{n=1}^{\infty} \int_{\varepsilon}^{L} (\omega *^k \omega)(x+2nL)\,\mathrm{d}x &= \sum_{n=1}^{\infty} \int_{\varepsilon+2nL}^{L+2nL} (\omega *^k \omega)(x)\,\mathrm{d}x \\
&\leq \sum_{n=1}^{\infty} \int_{\varepsilon+2nL}^{\infty} (\omega *^k \omega)(x)\,\mathrm{d}x \\
&\leq \sum_{n=1}^{\infty} \int_{2nL}^{\infty} (\omega *^k \omega)(x)\,\mathrm{d}x \\
&\leq \sum_{n=1}^{\infty} \mathrm{e}^{k\alpha(nL)} \mathrm{e}^{-2(nL)^2},
\end{aligned} \tag{C.15}$$

where on the last step we use the Chernoff bound for each term with $\lambda = nL$.

In order to bound the second term on the right hand side of (C.14) we consider the following. From the Chernoff bound we get

$$\mathbb{P}(\omega \leq -L) = \mathbb{P}(-\omega \geq L) \leq \frac{\mathbb{E}[\mathrm{e}^{-\lambda\omega}]}{\mathrm{e}^{\lambda L}} \tag{C.16}$$

for all $\lambda > 0$.

Let us use again the notation of the proof of Lemma C.2, i.e., denote $f_X(t) = q\mu_1(t) + (1-q)\mu_0(t)$, where $\mu_0(t) = \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-t^2}{2\sigma^2}}$ and $\mu_1(t) = \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}}$, and $f_Y(t) = \mu_0(t)$. By change of variables $s = \mathcal{L}_{X/Y}(t)$, we see that

$$\mathbb{E}[\mathrm{e}^{-\lambda\omega}] = \int_{-\infty}^{\infty} \mathrm{e}^{-\lambda \log \frac{f_X(t)}{f_Y(t)}} f_X(t)\,\mathrm{d}t = \int_{-\infty}^{\infty} \left(\frac{f_Y(t)}{f_X(t)}\right)^{\lambda} f_X(t)\,\mathrm{d}t. \tag{C.17}$$

From [4, Corollary 7] it follows that for all $\lambda \geq 1$,

$$\int_{-\infty}^{\infty} \left(\frac{f_Y(t)}{f_X(t)}\right)^{\lambda} f_X(t)\,\mathrm{d}t \leq \int_{-\infty}^{\infty} \left(\frac{f_X(t)}{f_Y(t)}\right)^{\lambda} f_Y(t)\,\mathrm{d}t = \int_{-\infty}^{\infty} \left(\frac{f_X(t)}{f_Y(t)}\right)^{\lambda-1} f_X(t)\,\mathrm{d}t = \mathbb{E}[\mathrm{e}^{(\lambda-1)\omega}]. \tag{C.18}$$

I.e., from (C.17) and (C.18) we find that for any $\lambda \geq 1$ it holds

$$\mathbb{E}[\mathrm{e}^{-\lambda\omega}] \leq \mathbb{E}[\mathrm{e}^{(\lambda-1)\omega}] = \mathrm{e}^{\alpha(\lambda-1)}. \tag{C.19}$$

Using the bounds (C.16) and (C.19) we get for the second term on the right hand side of (C.14):

$$\begin{aligned}\sum_{n=1}^{\infty}\int_{\varepsilon}^{L}(\omega *^k \omega)(x-2nL)\,\mathrm{d}x &= \sum_{n=1}^{\infty}\int_{\varepsilon-2nL}^{(1-2n)L}(\omega *^k \omega)(x)\,\mathrm{d}x\\ &\leq \sum_{n=1}^{\infty}\int_{-\infty}^{-(2n-1)L}(\omega *^k \omega)(x)\,\mathrm{d}x \\ &\leq \sum_{n=1}^{\infty}\mathrm{e}^{k\alpha(nL)}\mathrm{e}^{-2(nL)^2},\end{aligned} \tag{C.20}$$

where on the last step we use the Chernoff bound for each term with $\lambda = nL+1$. Substituting (C.15) and (C.20) into (C.14), we see that

$$\int_{\varepsilon}^{L}|C_1(x)|\,\mathrm{d}x \leq 2\sum_{n=1}^{\infty}\mathrm{e}^{k\alpha(nL)}\mathrm{e}^{-2(nL)^2}. \tag{C.21}$$

Moreover,

$$\begin{aligned}\int_{\varepsilon}^{L}|C_2(x)|\,\mathrm{d}x &= \int_{\varepsilon}^{L}\int_{-L}^{L}\omega(t_1)\ldots\int_{-L}^{L}\omega(t_{k-1})r(x-\textstyle\sum_{i=1}^{k-1}t_i)\,\mathrm{d}t_1\ldots\mathrm{d}t_{k-1}\,\mathrm{d}x\\ &= \int_{-L}^{L}\omega(t_1)\ldots\int_{-L}^{L}\omega(t_{k-1})\int_{\varepsilon}^{L}r(x-\textstyle\sum_{i=1}^{k-1}t_i)\,\mathrm{d}x\,\mathrm{d}t_1\ldots\mathrm{d}t_{k-1}.\end{aligned} \tag{C.22}$$

Clearly, for the inner factor in the integrand it holds by the Chernoff bound (setting $\lambda = L/2$)

$$\int_{\varepsilon}^{L}r(x-\textstyle\sum_{i=1}^{k-1}t_i)\,\mathrm{d}x \leq \displaystyle\int_{L}^{\infty}\omega(t)\,\mathrm{d}t \leq \mathrm{e}^{\alpha(L/2)}\mathrm{e}^{-\frac{L^2}{2}}.$$

Thus, from (C.22) it follows that

$$\int_{\varepsilon}^{L}|C_2(x)|\,\mathrm{d}x \leq \mathrm{e}^{\alpha(L/2)}\mathrm{e}^{-\frac{L^2}{2}}. \tag{C.23}$$

Substituting (C.21) and (C.23) into (C.13), we get

$$\int_{\varepsilon}^{L}\left|(\omega \circledast^k \omega - \widetilde{\omega}\circledast^k\widetilde{\omega})(x)\right|\,\mathrm{d}x \leq \mathrm{e}^{\alpha(L/2)}\mathrm{e}^{-\frac{L^2}{2}} + 2\sum_{n=1}^{\infty}\mathrm{e}^{k\alpha(nL)}\mathrm{e}^{-2(nL)^2}.$$

□

C.3 Error expansion with respect to Δx

The purpose of this section is to show that the following assumption used in the main text holds (recall $\Delta x = 2L/n$):

There exists a constant K independent of n such that

$$\int_{\varepsilon}^{L} (1 - \mathrm{e}^{\varepsilon - s})(\widetilde{\omega} \circledast^k \widetilde{\omega})(s)\,\mathrm{d}s - \Delta x \sum_{\ell=0}^{n-1} \big(1 - \mathrm{e}^{\varepsilon - (\ell \Delta x)}\big) C_\ell^k = K\Delta x + O\big((\Delta x)^2\big). \tag{C.24}$$

We motivate this assumption using the Euler–Maclaurin summation formula which gives the following expansion for the error of the Riemann sum formula (see [6, Ch. 3.3]).

Lemma C.7 (Euler–Maclaurin formula)**.** *Let $f \in C^{2m+2}[a,b]$. Let $N \in \mathbb{N}^+$ and denote $\Delta x = (b-a)/N$. Then,*

$$\Delta x \sum_{i=0}^{N-1} f(a + i\Delta x) - \int_a^b f(x)\,\mathrm{d}x = \Delta x \frac{f(a) - f(b)}{2} + \sum_{\ell=1}^{m} (\Delta x)^{2\ell} \frac{B_{2\ell}}{(2\ell)!} \big(f^{(2\ell-1)}(b) - f^{(2\ell-1)}(a)\big) + (\Delta x)^{2m+2} \frac{B_{2m+2}}{(2m+2)!} f^{(2m+2)}(\eta), \quad \eta \in [a,b],$$

where B_i is the ith Bernoulli number.

Consider the discrete convolution vector C^k as defined in Section 5. By definition (summations periodic, indices modulo n),

$$C_i^k = \Delta x \sum_{j=0}^{n-1} \widetilde{\omega}(j\Delta x) C_{i-j}^{k-1}, \quad C_i^2 = \Delta x \sum_{j=0}^{n-1} \widetilde{\omega}(j\Delta x)\widetilde{\omega}(i\Delta x - j\Delta x)$$

If, instead, we consider the discrete convolutions

$$\widehat{C}_i^k = \Delta x \sum_{j=0}^{n-1} \omega(j\Delta x) C_{i-j}^{k-1}, \quad \widehat{C}_i^2 = \Delta x \sum_{j=0}^{n-1} \omega(j\Delta x)\omega(i\Delta x - j\Delta x),$$

then by the Euler–Maclaurin formula there clearly exist a constant K independent of n such that

$$\widehat{C}_i^k - (\omega \circledast^k \omega)(-L + i\Delta x) = K\Delta x + O\big((\Delta x)^2\big)$$

for all $k = 1, \ldots$ and $i = 0, 1, \ldots, n-1$. Since the integrands in the convolution integrals of $\omega \circledast^k \omega$ are piecewise smooth (we omit details here), it also has to hold

$$C_i^k - (\widetilde{\omega} \circledast^k \widetilde{\omega})(-L + i\Delta x) = K\Delta x + O\big((\Delta x)^2\big) \tag{C.25}$$

for some constant K independent of n.

Using (C.25) and the Euler–Maclaurin formula and the fact that the expressions in (C.24) are piecewise smooth, verifies the assumption (C.24).

D Auxiliary results

The following lemma is needed in the derivation of Newton's iteration.

Lemma D.1. *Let*

$$f(\varepsilon) = \int_{\varepsilon}^{\infty} (1 - \mathrm{e}^{\varepsilon - s}) g(s) \, \mathrm{d}s.$$

Then,

$$f'(\varepsilon) = -\int_{\varepsilon}^{\infty} \mathrm{e}^{\varepsilon - s} g(s) \, \mathrm{d}s.$$

Proof. Writing

$$f(\varepsilon) = \int_{\varepsilon}^{\infty} g(s) \, \mathrm{d}s - \mathrm{e}^{\varepsilon} \int_{\varepsilon}^{\infty} \mathrm{e}^{-s} g(s) \, \mathrm{d}s$$

and using the fundamental theorem of calculus and the chain rule, we see that

$$f'(\varepsilon) = -g(\varepsilon) - \mathrm{e}^{\varepsilon} \int_{\varepsilon}^{\infty} \mathrm{e}^{-s} g(s) \, \mathrm{d}s + \mathrm{e}^{\varepsilon} \cdot \mathrm{e}^{-\varepsilon} g(\varepsilon) = -\int_{\varepsilon}^{\infty} \mathrm{e}^{\varepsilon - s} g(s) \, \mathrm{d}s.$$

□

Recall that for the error analysis we consider the neighbouring relation $\sim_R$, i.e., we consider the density function

$$\omega(s) = \begin{cases} f(g(s))g'(s), & \text{if } s > \log(1-q), \\ 0, & \text{otherwise,} \end{cases}$$

where

$$f(t) = \frac{1}{\sqrt{2\pi\sigma^2}} [q\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\mathrm{e}^{-\frac{t^2}{2\sigma^2}}], \tag{D.1}$$

$$g(s) = \sigma^2 \log \left(\frac{\mathrm{e}^s - (1-q)}{q} \right) + \frac{1}{2}. \tag{D.2}$$

The following lemmas which are be needed in the analysis of the approximation error.

Lemma D.2. *For all* $s \in (\log(1-q), \infty)$*:*

$$\omega(s) \leq \frac{\sigma}{q\sqrt{2\pi}} \mathrm{e}^{\frac{1}{\sigma^2}}.$$

Proof. Consider first the case $s \in (\log(1-q), 0]$. We see that then $g(s) \in (-\infty, \frac{1}{2}]$ and therefore

$$\mathrm{e}^{-\frac{(g(s)-1)^2}{2\sigma^2}} \leq \mathrm{e}^{-\frac{g(s)^2}{2\sigma^2}}.$$

Thus,

$$f(g(s)) \leq \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\frac{g(s)^2}{2\sigma^2}}. \tag{D.3}$$

Moreover, for all $s \in (\log(1-q), 0]$,

$$g'(s) = \frac{\sigma^2 \mathrm{e}^s}{\mathrm{e}^s - (1-q)} \leq \frac{\sigma^2}{\mathrm{e}^s - (1-q)}. \tag{D.4}$$

Using (D.3) and (D.4), we find that

$$\omega(s) \leq \frac{\sigma}{\sqrt{2\pi}} \frac{\mathrm{e}^{-\frac{g(s)^2}{2\sigma^2}}}{\mathrm{e}^s - (1-q)}. \tag{D.5}$$

We make the change of variables $x = g(s)$. Then,

$$\frac{1}{\mathrm{e}^s - (1-q)} = q^{-1}\, \mathrm{e}^{\frac{-2x+1}{2\sigma^2}}$$

and from (D.5) we see that

$$\omega(s) \leq \frac{\sigma}{q\sqrt{2\pi}} \mathrm{e}^{\frac{-x^2}{2\sigma^2}}\, \mathrm{e}^{\frac{-2x+1}{2\sigma^2}} = \frac{\sigma}{q\sqrt{2\pi}} \mathrm{e}^{\frac{1}{\sigma^2}}\, \mathrm{e}^{\frac{-(x+1)^2}{2\sigma^2}} \leq \frac{\sigma}{q\sqrt{2\pi}} \mathrm{e}^{\frac{1}{\sigma^2}}$$

which shows the claim for $s \in (\log(1-q), 0]$.

Assume next $s \geq 0$. Then,

$$g'(s) = \frac{\sigma^2 \mathrm{e}^s}{\mathrm{e}^s - (1-q)} = \frac{\sigma^2}{1 - \frac{1-q}{\mathrm{e}^s}} \leq \frac{\sigma^2}{q}.$$

Since $f(g(s)) \leq \frac{1}{\sqrt{2\pi\sigma^2}}$, we see that when $s > 0$,

$$\omega(s) \leq \frac{\sigma}{q\sqrt{2\pi}}.$$

□

Lemma D.3. *For all* $s \geq 1$ *and* $0 < q \leq \frac{1}{2}$*:*

$$\omega(s) \leq \sigma \mathrm{e}^{-\frac{-(\sigma^2 s + C)^2}{2\sigma^2}},$$

where $C = \sigma^2 \log(\frac{1}{2q}) - \frac{1}{2}$.

Proof. Since $s \geq 1$,

$$\mathrm{e}^s - (1-q) \geq \frac{1}{2}\mathrm{e}^s$$

and therefore

$$g(s) = \sigma^2 \log\left(\frac{\mathrm{e}^s - (1-q)}{q}\right) + \frac{1}{2} \geq \sigma^2 s + C,$$

where $C = \sigma^2 \log(\frac{1}{2q}) + \frac{1}{2}$. We see that $C \geq \frac{1}{2}$, since $0 < q \leq \frac{1}{2}$. Then also

$$f(g(s)) \leq \frac{1}{\sqrt{2\pi\sigma^2}}\mathrm{e}^{-\frac{-(\sigma^2 s + C)^2}{2\sigma^2}},$$

Furthermore, when $s > 1$,

$$g'(s) = \frac{\sigma^2 \mathrm{e}^s}{\mathrm{e}^s - (1-q)} \leq 2\sigma^2.$$

Thus, when $s > 1$,

$$\omega(s) \leq \sigma\sqrt{\frac{2}{\pi}}\mathrm{e}^{-\frac{-(\sigma^2 s + C_2)^2}{2\sigma^2}} \leq \sigma \mathrm{e}^{-\frac{-(\sigma^2 s + C_2)^2}{2\sigma^2}}.$$

□

D.1 Bounds for derivatives

Lemma D.4. *Suppose $\sigma \geq 1$. For all $s \in (\log(1-q), \infty)$:*

$$\left|\omega'(s)\right| \leq 4\mathrm{e}^{\frac{3}{\sigma^2}}\frac{\sigma^3}{q^2}$$

and

$$\left|\omega''(s)\right| \leq 11\mathrm{e}^{\frac{9}{2\sigma^2}}\frac{\sigma^3}{q^3}.$$

Proof. Denote

$$\omega(s) = f(g(s))g'(s),$$

where

$$g(s) = \sigma^2 \log\left(\frac{\mathrm{e}^s - (1-q)}{q}\right) + \frac{1}{2} \tag{D.6}$$

and

$$f(t) = \frac{1}{\sqrt{2\pi\sigma^2}}[q\mathrm{e}^{\frac{-(t-1)^2}{2\sigma^2}} + (1-q)\mathrm{e}^{-\frac{t^2}{2\sigma^2}}].$$

Straightforward calculation shows that

$$\omega'(s) = f'(g(s))(g'(s))^2 + f(g(s))g''(s) \tag{D.7}$$

and

$$\omega^{(2)}(s) = f''(g(s))(g'(s))^3 + 3f'(g(s))g''(s)g'(s) + f(g(s))g^{(3)}(s). \tag{D.8}$$

Moreover,

$$\begin{aligned} g'(s) &= \frac{\sigma^2 \mathrm{e}^s}{\mathrm{e}^s - (1-q)}, \\ g''(s) &= -\frac{\sigma^2(1-q)\mathrm{e}^s}{\big(\mathrm{e}^s - (1-q)\big)^2}, \\ g^{(3)}(s) &= \frac{\sigma^2(1-q)\mathrm{e}^s(\mathrm{e}^s + (1-q))}{\big(\mathrm{e}^s - (1-q)\big)^3}. \end{aligned} \tag{D.9}$$

Case $s \geq 0$. When $s \geq 0$, it holds

$$\frac{\mathrm{e}^s}{\mathrm{e}^s - (1-q)} = \frac{1}{1 - \frac{1-q}{\mathrm{e}^s}} \leq \frac{1}{q}$$

and from this inequality and expressions (D.9) it follows that

$$\begin{aligned} \left|g'(s)\right| &\leq \frac{\sigma^2}{q}, \\ \left|g''(s)\right| &\leq \frac{\sigma^2}{q^2}, \\ \left|g^{(3)}(s)\right| &\leq \frac{2\sigma^2}{q^3}. \end{aligned} \tag{D.10}$$

Notice that when $s \geq 0$, $g(s) \geq \frac{1}{2}$. By an elementary calculus, we find that when $\sigma \geq 1$, for $t \geq \frac{1}{2}$ it holds

$$\begin{aligned} f(t) &\leq \frac{1}{\sigma}, \\ f'(t) &\leq \frac{1}{\sqrt{2\pi\sigma^2}} \frac{t}{\sigma} \mathrm{e}^{-\frac{(t-1)^2}{2\sigma^2}} \leq \frac{1}{\sigma} \\ f''(t) &\leq \frac{1}{\sqrt{2\pi\sigma^2}} \left(\frac{t^2}{\sigma^2} + \frac{1}{\sigma^2}\right) \mathrm{e}^{-\frac{(t-1)^2}{2\sigma^2}} \leq \frac{2}{\sigma^3}. \end{aligned} \tag{D.11}$$

Substituting (D.11) and (D.10) into (D.7) and (D.8) we find that

$$\begin{aligned} \left|\omega'(s)\right| &\leq 2\frac{\sigma^3}{q^2}, \\ \left|\omega''(s)\right| &\leq 7\frac{\sigma^3}{q^3}. \end{aligned} \tag{D.12}$$

when $s \geq 0$.

Case $s \in (\log(1-q, 0))$. When $s \in (\log(1-q), 0)$, from (D.9) it follows that

$$\begin{aligned}
\left|g'(s)\right| &\leq \frac{\sigma^2}{\mathrm{e}^s - (1-q)}, \\
\left|g''(s)\right| &\leq \frac{\sigma^2}{\big(\mathrm{e}^s - (1-q)\big)^2}, \\
\left|g^{(3)}(s)\right| &\leq \frac{2\sigma^2}{\big(\mathrm{e}^s - (1-q)\big)^3}.
\end{aligned} \tag{D.13}$$

Consider next the five terms on the right hand sides of (D.7) and (D.8). Consider first the term $f(g(s))g''(s)$. By (D.13), we have the bound

$$f(g(s))g''(s) \leq f(g(s)) \frac{\sigma^2}{\big(\mathrm{e}^s - (1-q)\big)^2}. \tag{D.14}$$

Next, make the change of variables $x = g(s)$. Then, since (see (D.6))

$$\frac{1}{\mathrm{e}^s - (1-q)} = q^{-1}\,\mathrm{e}^{\frac{-2x+1}{2\sigma^2}}, \tag{D.15}$$

the bound (D.14) gives

$$f(g(s))g''(s) \leq \sigma^2 q^{-2} f(x) \mathrm{e}^{\frac{-4x+2}{2\sigma^2}} \leq \sigma^2 q^{-2} \mathrm{e}^{\frac{3}{\sigma^2}} \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{\frac{-(x+2)^2}{2\sigma^2}} \leq \frac{1}{\sqrt{2\pi}} \mathrm{e}^{\frac{3}{\sigma^2}} \frac{\sigma}{q^2}, \tag{D.16}$$

as $f(t) \leq \frac{1}{\sqrt{2\pi\sigma^2}} \mathrm{e}^{\frac{-t^2}{2\sigma^2}}$ for $t \leq \frac{1}{2}$ and $g(s) \leq \frac{1}{2}$ for $s \in (\log(1-q, 0))$. With a similar technique, i.e., by using the change of variables $x = g(s)$ and (D.15), we find after tedious calculation that

$$\begin{aligned}
f'(g(s))\big(g'(s)\big)^2 &\leq 3\mathrm{e}^{\frac{3}{\sigma^2}} \frac{\sigma^3}{q^2}, \\
f''(g(s))\big(g'(s)\big)^3 &\leq 6\mathrm{e}^{\frac{9}{2\sigma^2}} \frac{\sigma^3}{q^3}, \\
3f'(g(s))g''(s)g'(s) &\leq 4\mathrm{e}^{\frac{9}{2\sigma^2}} \frac{\sigma^3}{q^3}, \\
f(g(s))g^{(3)}(s) &\leq \frac{1}{\sqrt{2\pi}} \mathrm{e}^{\frac{9}{2\sigma^2}} \frac{\sigma}{q^3}.
\end{aligned} \tag{D.17}$$

Substituting (D.16) and (D.17) into (D.7) and (D.8) gives the bounds

$$\begin{aligned} \left|\omega'(s)\right| &\leq 4\mathrm{e}^{\frac{3}{\sigma^2}}\frac{\sigma^3}{q^2}, \\ \left|\omega''(s)\right| &\leq 11\mathrm{e}^{\frac{9}{2\sigma^2}}\frac{\sigma^3}{q^3} \end{aligned} \tag{D.18}$$

for all $s \in (\log(1-q, 0))$.

The claim follows from the bounds (D.12) and (D.18).

□

D.2 Tables of numerical convergence for Section 8

n	FA	$\text{err}(L,n)$
$5 \cdot 10^4$	0.0491228786423	$2.01 \cdot 10^{-2}$
$1 \cdot 10^5$	0.0496089458356	$3.12 \cdot 10^{-4}$
$2 \cdot 10^5$	0.0496013846114	$1.06 \cdot 10^{-6}$
$4 \cdot 10^5$	0.0496014103882	$1.71 \cdot 10^{-9}$
$8 \cdot 10^5$	0.0496014103252	$2.66 \cdot 10^{-11}$
$1.6 \cdot 10^6$	0.0496014103146	$8.88 \cdot 10^{-12}$
$3.2 \cdot 10^6$	0.0496014103163	$2.22 \cdot 10^{-12}$

Table 1: Convergence of $\delta(\varepsilon)$-approximation with respect to n (when $L = 12$) and the estimate (7.4). The tail bound estimate (7.3) is $O(10^{-24})$.

L	FA	estimate (7.3)
2.0	0.0422160172923	$3.32 \cdot 10^{-1}$
4.0	0.0496008932869	$4.96 \cdot 10^{-3}$
6.0	0.0496014103158	$3.32 \cdot 10^{-6}$
8.0	0.0496014103134	$1.00 \cdot 10^{-10}$
10.0	0.0496014103134	$1.36 \cdot 10^{-16}$
12.0	0.0496014103163	$8.30 \cdot 10^{-24}$

Table 2: Convergence of the $\delta(\varepsilon)$-approximation with respect to L (when $n = 3.2 \cdot 10^6$) and the error estimate (7.3). The estimate $\text{err}(L,n) = O(10^{-12})$.

References

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proc. CCS 2016*, 2016.

[2] Borja Balle, Gilles Barthe, and Marco Gaboardi. Privacy amplification by subsampling: Tight analyses via couplings and divergences. In *Advances in Neural Information Processing Systems*, pages 6277–6287, 2018.

[3] Sebastian Meiser and Esfandiar Mohammadi. Tight on budget?: Tight bounds for r-fold approximate differential privacy. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 247–264. ACM, 2018.

[4] Ilya Mironov, Kunal Talwar, and Li Zhang. Rényi differential privacy of the sampled gaussian mechanism. *arXiv preprint arXiv:1908.10530*, 2019.

[5] David M Sommer, Sebastian Meiser, and Esfandiar Mohammadi. Privacy loss classes: The central limit theorem in differential privacy. *Proceedings on Privacy Enhancing Technologies*, 2019(2):245–269, 2019.

[6] Josef Stoer and Roland Bulirsch. *Introduction to numerical analysis*, volume 12. Springer Science & Business Media, 2013.

[7] Martin J Wainwright. *High-dimensional statistics: A non-asymptotic viewpoint*, volume 48. Cambridge University Press, 2019.

[8] Yu-Xiang Wang, Borja Balle, and Shiva Kasiviswanathan. Subsampled Rényi differential privacy and analytical moments accountant. In *Proc. AISTATS 2019*, 2019.