Additional Experiment Results

1 Comparison in Pure Differential Privacy Settings

Consider the pure differential privacy setting, where $\Delta = \delta = 0$. Consider $K = 11$, $\epsilon = 0.1$ and $m \in \{1, 3, 5, 7, 9, 11\}$.

We compare four different γ noise functions:

1. γ_{opt} (Ours): optimized γ function using our optimization framework from Section 6
2. γ_{Sub} (Baseline): the γ function that corresponds to outputting the majority of m out K subsampled mechanisms
3. γ_{DSub} (Baseline): the γ function that corresponds to outputting $2m-1$ subsampled mechanisms from Theorem 4.1, aka., Double Subsampling (DSub)
4. γ_{const} (Baseline): the constant γ function that corresponds to the classical Randomized Response (RR) algorithm

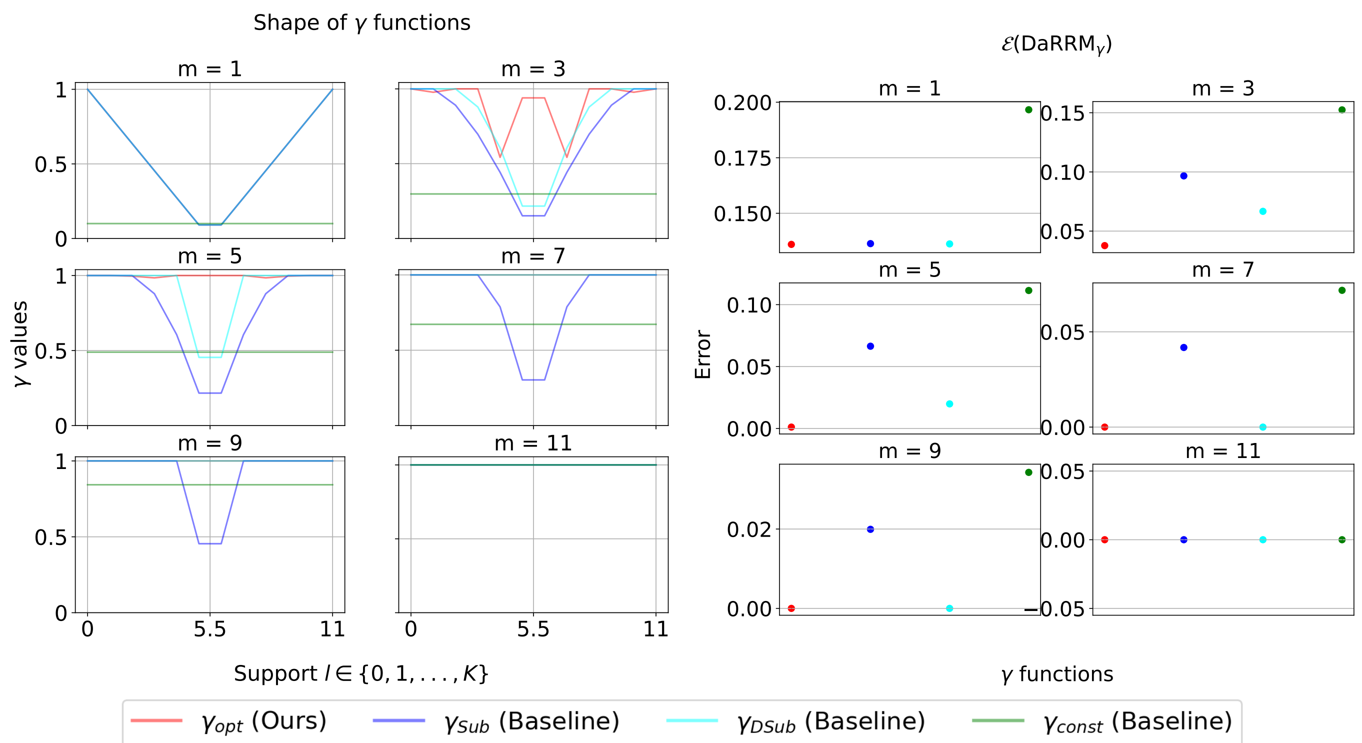

Figure 1: Plots of shape and $\mathcal{E}(\mathsf{DaRRM}_\gamma)$ of different γ functions: the optimized γ_{Opt}, the baselines γ_{Sub} and γ_{DSub} (Theorem 4.1), and the constant γ_{const} (in RR). Here, $K = 11, m \in \{1, 3, 5, 7, 9, 11\}$, $\epsilon = 0.1$ and $\delta = \Delta = 0$. Note when $m \in \{7, 9\}$, the cyan line (γ_{DSub}) and the red line (γ_{opt}) overlap. When $m = 11$, all lines overlap. Observe that when $m \geq \frac{K+1}{2}$, that is, $m \in \{7, 9, 11\}$ in this case, the above plots suggest both γ_{opt} and γ_{DSub} achieve the minimum error at 0. This is consistent with our theory.

2 Additional Results for Private Semi-Supervised Knowledge Transfer

$m = 1$.

Dataset	# Queries	Privacy loss per query $(m\epsilon, m\Delta)$	Total privacy loss over Q queries $(\epsilon_{total}, \delta_{total})$
MNIST	$Q = 20$	$(0.0892, 0.0001)$	$(1.88, 0.002)$
	$Q = 50$		$(3.12, 0.005)$
	$Q = 100$		$(4.66, 0.010)$
Fashion MNIST	$Q = 20$	$(0.0852, 0.0001)$	$(1.79, 0.002)$
	$Q = 50$		$(2.96, 0.005)$
	$Q = 100$		$(4.41, 0.010)$

Table 1: The privacy loss per query to the teachers and the total privacy loss over Q queries. Note the total privacy loss is computed by advanced composition, where $\delta_{total} = Q\delta + \delta'$ for some $\delta' > 0$. Here, $\delta' = 0.0001$.

Dataset	MNIST			Dataset	Fashion-MNIST		
# Queries	GNMax (Baseline)	DaRRM$_{\gamma_{Sub}}$ (Baseline)	DaRRM$_{\gamma_{opt}}$ (Ours)	# Queries	GNMax (Baseline)	DaRRM$_{\gamma_{Sub}}$ (Baseline)	DaRRM$_{\gamma_{opt}}$ (Ours)
$Q = 20$	0.54 (0.09)	**0.71 (0.08)**	0.68 (0.07)	$Q = 20$	0.45 (0.10)	**0.92 (0.06)**	0.90 (0.07)
$Q = 50$	0.56 (0.10)	0.71 (0.05)	**0.72 (0.05)**	$Q = 50$	0.59 (0.04)	0.88 (0.03)	**0.89 (0.04)**
$Q = 100$	0.56 (0.05)	0.68 (0.06)	**0.71 (0.04)**	$Q = 100$	0.55 (0.06)	0.90 (0.02)	**0.91 (0.03)**

Table 2: Accuracy of the predicted labels of Q query samples on datasets MNIST (on the left) and Fashion-MNIST (on the right). We report the mean and one std. in parentheses over 10 random draws of the query samples from the test dataset. Note each prediction on the query sample is $(m\epsilon, \delta)$-differentially private. With the same per query privacy loss (and hence the same total privacy loss over Q samples), DaRRM$_{\gamma_{opt}}$ achieves the highest accuracy compared to the other two baselines.

$m = 5$.

Dataset	# Queries	Privacy loss per query $(m\epsilon, m\Delta)$	Total privacy loss over Q queries $(\epsilon_{total}, \delta_{total})$
MNIST	$Q = 20$	$(0.4460, 0.0005)$	$(13.57, 0.010)$
	$Q = 50$		$(26.07, 0.025)$
	$Q = 100$		$(44.21, 0.050)$
Fashion MNIST	$Q = 20$	$(0.4260, 0.0005)$	$(12.70, 0.010)$
	$Q = 50$		$(24.24, 0.025)$
	$Q = 100$		$(40.91, 0.050)$

Table 3: The privacy loss per query to the teachers and the total privacy loss over Q queries. Note the total privacy loss is computed by advanced composition, where $\delta_{total} = Q\delta + \delta'$ for some $\delta' > 0$. Here, $\delta' = 0.0001$.

Dataset	MNIST			Dataset	Fashion-MNIST		
# Queries	GNMax (Baseline)	$\mathsf{DaRRM}_{\gamma_{Sub}}$ (Baseline)	$\mathsf{DaRRM}_{\gamma_{opt}}$ (Ours)	# Queries	GNMax (Baseline)	$\mathsf{DaRRM}_{\gamma_{Sub}}$ (Baseline)	$\mathsf{DaRRM}_{\gamma_{opt}}$ (Ours)
$Q = 20$	0.72 (0.11)	0.81 (0.10)	**0.86 (0.06)**	$Q = 20$	0.73 (0.11)	0.97 (0.03)	**0.98 (0.02)**
$Q = 50$	0.74 (0.06)	0.79 (0.07)	**0.82 (0.03)**	$Q = 50$	0.69 (0.07)	**0.96 (0.04)**	**0.96 (0.04)**
$Q = 100$	0.73 (0.06)	0.77 (0.04)	**0.82 (0.04)**	$Q = 100$	0.73 (0.03)	0.96 (0.03)	**0.97 (0.03)**

Table 4: Accuracy of the predicted labels of Q query samples on datasets MNIST (on the left) and Fashion-MNIST (on the right). We report the mean and one std. in parentheses over 10 random draws of the query samples from the test dataset. Note each prediction on the query sample is $(m\epsilon, \delta)$-differentially private. With the same per query privacy loss (and hence the same total privacy loss over Q samples), $\mathsf{DaRRM}_{\gamma_{opt}}$ achieves the highest accuracy compared to the other two baselines.

$m = 7$.

Dataset	# Queries	Privacy loss per query $(m\epsilon, m\Delta)$	Total privacy loss over Q queries $(\epsilon_{total}, \delta_{total})$
MNIST	$Q = 20$	$(0.6244, 0.0007)$	$(22.81, 0.014)$
	$Q = 50$		$(46.02, 0.035)$
	$Q = 100$		$(80.94, 0.070)$
Fashion MNIST	$Q = 20$	$(0.5964, 0.0007)$	$(21.18, 0.014)$
	$Q = 50$		$(42.42, 0.035)$
	$Q = 100$		$(74.24, 0.070)$

Table 5: The privacy loss per query to the teachers and the total privacy loss over Q queries. Note the total privacy loss is computed by advanced composition, where $\delta_{total} = Q\delta + \delta'$ for some $\delta' > 0$. Here, $\delta' = 0.0001$.

Dataset	MNIST			Dataset	Fashion-MNIST		
# Queries	GNMax (Baseline)	$\mathsf{DaRRM}_{\gamma_{Sub}}$ (Baseline)	$\mathsf{DaRRM}_{\gamma_{opt}}$ (Ours)	# Queries	GNMax (Baseline)	$\mathsf{DaRRM}_{\gamma_{Sub}}$ (Baseline)	$\mathsf{DaRRM}_{\gamma_{opt}}$ (Ours)
$Q = 20$	0.84 (0.08)	0.85 (0.06)	**0.86 (0.07)**	$Q = 20$	0.78 (0.10)	**0.97 (0.02)**	**0.97 (0.02)**
$Q = 50$	**0.82 (0.06)**	0.77 (0.07)	**0.82 (0.07)**	$Q = 50$	0.79 (0.07)	0.96 (0.03)	**0.97 (0.02)**
$Q = 100$	0.80 (0.04)	0.82 (0.03)	**0.84 (0.03)**	$Q = 100$	0.82 (0.03)	0.97 (0.02)	**0.98 (0.02)**

Table 6: Accuracy of the predicted labels of Q query samples on datasets MNIST (on the left) and Fashion-MNIST (on the right). We report the mean and one std. in parentheses over 10 random draws of the query samples from the test dataset. Note each prediction on the query sample is $(m\epsilon, \delta)$-differentially private. With the same per query privacy loss (and hence the same total privacy loss over Q samples), $\mathsf{DaRRM}_{\gamma_{opt}}$ achieves the highest accuracy compared to the other two baselines.