CS848 Winter 2021 Assignment 2

[TODO]: [Student Name]

Due by March 1, 11pm

Please submit a pdf solution on Learn: "Submit" → "Dropbox folder" → "Assignment 2".

Q1. Randomized Response

Consider a domain $\Sigma = \{l_1, \ldots, l_k\}$ of k locations, please design a randomized response R that takes in a true location $l \in \Sigma$ and randomly outputs a location $o \in \Sigma$.

(a) Privacy Guarantee

[5 points] Please describe your algorithm and show that the algorithm achieves ϵ-local differential privacy.
[TODO]: Add your description and privacy proof here. Pseudo code or diagrams or bullet points are all acceptable.

(b) Utility Guarantee

[5 points] Suppose N people in the dataset and n_{l_i} denote the number of people who are at location l_i. Each person applies the randomized response proposed by you. Among these noise responses there are $\tilde{n}_{l_1}$ number of people reported location $l_1 \in \Sigma$. Please show an unbiased estimator $\hat{n}_{l_1}$ for the true number of people who are actually at location l_1, i.e. $E[\hat{n}_{l_1}] = n_{l_1}$,
[TODO]: Show your expression for $\hat{n}_{l_1}$ and why it is unbiased.

Q2. 1-out-of-k Oblivious Transfer

In the lecture, we cover how to use public encryption to construct a 1-out-of-2 oblivious transfer protocol.

(a) Problem Description

[5 points] Describe the problem of 1-out-of-k oblivious transfer for 2 parties.
[TODO]: Add your description here.

(b)Protocol Description

[5 points] Describe one possible way to solve the problem above (e.g. similar as the public encryption used for 1-out-of-2 OT in the lecture) and briefly justify it.
[TODO]: Add your description here.