第四次作业

2（1）

1.**数据准备：** 收集用户Ui的历史用电量数据$Ri^((t))$，并将数据按照时间顺序排序。

2.**噪声引入：**对每个用户Ui在t时刻的真实用电量$Ri^((t))$，应用拉普拉斯机制，生成带有噪声的用电量数据。

$$P(x \mid b)=\frac{1}{2b}exp(-\frac{|x|}{b})$$
$$=\frac{1}{2b}exp(-\frac{\epsilon\,|x|}{\Delta f})$$

对于每个用户U_i，加噪声后的用电量数据为：

$$\hat{R}_i^{(t)}=R_i^{(t)}+Laplace(0,b)$$

3.**构建模型：**

使用带有噪声的数据训练负荷预测模型。在训练过程中，梯度更新的时候，需要在梯度中添加拉普拉斯噪声，以确保差分隐私。

$$NoisyGradient=TrueGradient+Laplace(0,\frac{\Delta f}{\epsilon})$$

4.**使用模型预测用电负荷**

2（2）

1.**初始模型分发：** 数据分析平台训练一个初始的负荷预测模型w，并使用差分隐私技术保护模型的参数。然后，将该隐私保护的初始模型w 分发给用户U_i。

2.**本地训练：** 用户U_i在本地使用自己的用电量数据进行模型的进一步训练，而无需将真实用电量信息传输到数据分析平台。用户只需传输本地训练中生成的模型更新参数。训练中引入差分隐私机制，即在模型参数更新的时候，对梯度进行差分隐私处理。

$$NoisyGradient=TrueGradient+Laplace(0,\frac{\Delta f}{\epsilon})$$

3.**模型更新传输：** 用户将带有差分隐私处理的模型更新参数传输回数据分析平台，而不传输用户的原始用电量信息。

4.**使用模型预测用电负荷**