**Differentially Private Quantile Regression**

Cezareo Rodriguez1 and Michael Li2

1Washington University in St Louis; 2Newport High School, Bellevue, WA

Differential privacy is a statistical and cryptographic technique in which noise is added to a database or statistics to protect or reduce the impact on the privacy of individual information contained within the database. Under privacy constraints, this procedure aims to publish meaningful information about the database while limiting disclosure of private database information. In our study, we extend quantile regression to the differential privacy setting. To do this, we examine the effect of adding various noise on the level of accuracy of regression parameters and their effects on the sensitivity of the quantile regression estimator. Quantile regression is often used in cases of non-normality or heteroskedastic data, so the impact of these ordinary least squares model assumption violations are also investigated. Under these different scenarios, the operating characteristics of quantile regression are evaluated by simulations.