3.1 Privacy mechanism

Using the Laplace mechanism to release the noisy sufficient statistics z results in the model shown in Figure 1. This is the same model used in non-private linear regression except for the introduction of z, which requires the exact sufficient statistics s to have finite sensitivity. A standard assumption in literature [Awan and Slavkovic, 2018, Sheffet, 2017, Wang, 2018, Zhang et al., 2012] is to assume x and y have known a priori lower and upper bounds, $(a_{\mathbf{x}}, b_{\mathbf{x}})$ and (a_y, b_y), with bound widths $w_{\mathbf{x}} = b_{\mathbf{x}} - a_{\mathbf{x}}$ (assuming, for simplicity, equal bounds for all covariate dimensions) and $w_y = b_y - a_y$, respectively. We can then reason about the worst case influence of an individual on each component of $\mathrm{s} = [X^T X, X^T \mathrm{y}, \mathrm{y}^T \mathrm{y}]$, recalling that $\mathrm{s} = \sum_i t(\mathrm{x}^{(i)}, y^{(i)})$, so that $[\Delta_{(X^T X)_{jk}}, \Delta_{(Xy)_j}, \Delta_{y^2}] = [w_{\mathbf{x}}^2, w_{\mathbf{x}} w_y, w_y^2]$. The number of unique elements[2] in s is $[d(d+1)/2,\ d,\ 1]$, so $\Delta_{\mathbf{s}} = w_{\mathbf{x}}^2 d(d+1)/2 + w_{\mathbf{x}} w_y d + w_y^2$. The noisy sufficient statistics fit for public release are

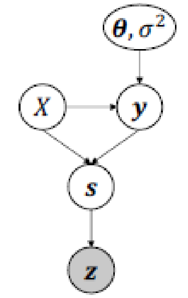

Figure 1: Private regression model.