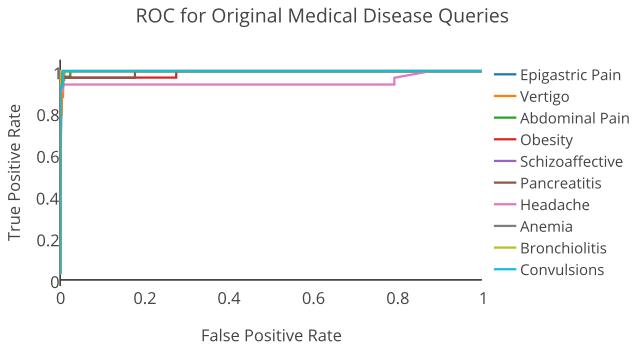

Figure 1: (Pre-obfuscation) Rate of true positives vs. false positives for classifying memory request traces of medical disease queries. Each query is for the average cost of different admitting patient diagnoses. This shows our modeled attacker's classification has near perfect accuracy when observing the original queries execution.

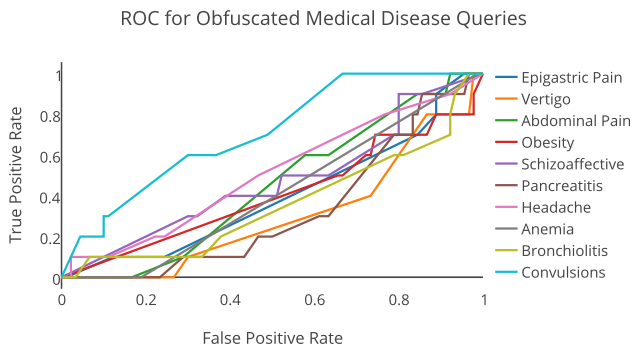

Figure 2: (Post-obfuscation) Rate of true positives vs. false positives for classifying obfuscated memory request traces of the same medical disease queries using a privacy parameter of $\epsilon = 0.1$. This shows our modeled attacker's classification is much more difficult after applying our obfuscation scheme.

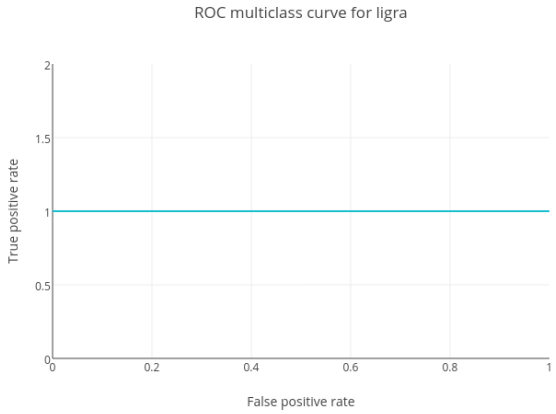

Figure 3: (Pre-obfuscation) Rate of true positives vs. false positives for classifying memory request of graph applications.

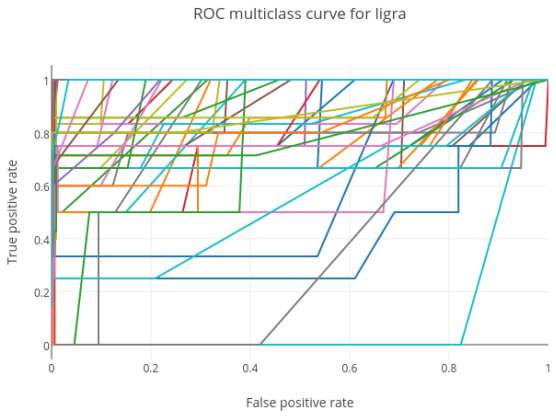

Figure 4: (Post-obfuscation) Rate of true positives vs. false positives for classifying obfuscated memory request traces of the same graph applications using a privacy parameter of $\epsilon = 1$. This shows our modeled attacker's classification is much more difficult after applying our obfuscation scheme.

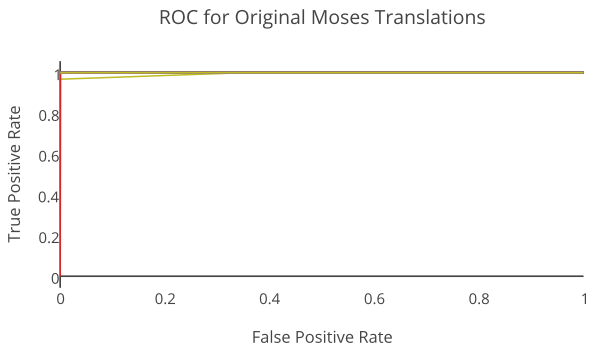

Figure 5: (Pre-obfuscation) Rate of true positives vs. false positives for classifying memory request traces of sentence translations. This shows our modeled attacker's classification has near perfect accuracy when observing the original queries execution.

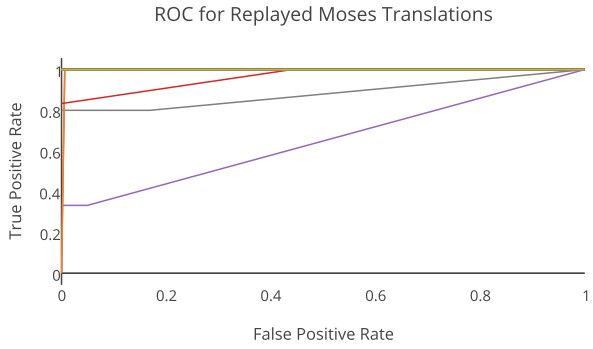

Figure 6: (Post-obfuscation) Rate of true positives vs. false positives for classifying obfuscated memory request traces of the same translations using a privacy using our replay model. This shows our modeled attacker's classification is much more difficult after applying our obfuscation scheme.