



## Status Report

Intern: Rito

Week 2 : 18<sup>th</sup> May, 2015 to 24<sup>th</sup> May, 2015

Number of hours worked: 25

Update: Working on migrating the security proof for the problem of 'back-dating' assuming that the information 'r' available to the adversary is quantum in nature. This work was expected to have a preliminary proof draft by the end of this week, but due to certain issues regarding migrating the definition of k-strong security and its applications to the quantum setting. These are now resolved, and a preliminary draft for the proof in a quantum setting, with additional notes and comments regarding areas which can be improved, should be ready and submitted by the middle of the next week and latest along with the report for Week 3 (next week).