guardtime

Status Report

Intern: Rito

Week 0 : 4th May, 2015 to 10th May, 2015

Number of hours worked: 25

Update: Mostly introductory work for the first week – trying to understand in detail how Guardtime functions and the structure that holds it together. Studied research papers in the public domain on Guardtime's technology, and understood the basic framework underneath, especially the algorithmic details. Exploring the areas of quantum information and post-quantum security proofs, in a possible attempt to formalize the corresponding proofs for KSI. Focusing on the areas of how a 'conventional' classical security proof can be morphed and adjusted to suit a quantum security setting, and how notions of classical security change in a quantum setting (some constraints may become redundant, other sufficient constraints may become insufficient.)