guardtime

Status Report

Intern: Rito

Week 1 : 11th May, 2015 to 17th May, 2015

Number of hours worked: 30

Update: Analyzed current security of KSI in a classical setting. To prove quantum-security of the same scheme, we need to go about it in a systematic manner. First, we analyze the strength of the underlying hash function. Then, assuming that our hash function being used is sufficiently secure for our purposes, we have to analyze the protocol in the usual way of having the adversary play games and finding his advantage. However, the current games need to be transformed (either preserved or updated) to a quantum setting. It may so happen that for the adversary to have negligible advantage for a particular game, we may need to tweak certain things to prove security. A more extensive report is attached in addition to the usual weekly status report, with comments, inputs and observations on the current state and how we should proceed.