guardtime

Status Report

Intern: Rito

Week 7: 22nd June, 2015 to 28th June, 2015

Number of hours worked: 25

Update:

We have updated the (as yet incomplete) proof to include the superposition capabilities of the adversary. In particular, we are trying to find out the parameters *t* and *s* to remain within bounds to fit the security we want to achieve. This is hard because it looks intuitively correct, but a formal proof is difficult and there is very little literature on how to proceed. Moreover, all existing proofs of quantum-immunity relies ultimately on the quantum-security of the underlying primitive of the hash function, and it is difficult to reduce this particular case to a manipulated and modified functional form of the same primitive.

Additional Note: As referenced in a previous report, the paper by Katz is absolutely not of any use, in fact I wrote an e-mail to the author pointing out the deficiencies and contradictions and possible counter-measures, to which he has not replied.