guardtime

Status Report

Intern: Rito

Week 4: 1st June to 7th June, 2015

Number of hours worked: 25

Update:

Following the definition of a two-stage adversary as defined in the paper [1] by Ahto Buldas and Risto Lanojaa at ACISP 2008, we have now reached a formal definition of the scenario in a quantum setting. For generating the hash chain, the auxiliary information made available in the second stage is quantum, and this has a wide range of implications, including on the related definition of minimum entropy. Instead of following the standard model of a random oracle, we will assume that there is no reason not to think that the adversary cannot instantiate, for himself, a concrete function.

Naturally, as noted by Song in his paper, we will henceforth consider that the adversary *can* query the oracle or the extractor in quantum superposition.

This is a significant change from our previous stance, and I will be contacting my advisors at GuardTime for some headstart in this direction.