guardtime

Status Report

Intern: Rito

Week 5: 8th June, 2015 to 15th June, 2015

Number of hours worked: 25

Update:

The class-respectful reduction that we are trying to *preserve* fails under the consideration that the query may be made in quantum superposition. This week's work has therefore not made any progress in the sense that we have not moved towards achieving the security proof needed. However, it has pointed out several flaws and inconsistencies.

In particular, in the extractor, there are several errata – or rather, inconsistencies – in the working of the extractor in a quantum environment, as published in [4]. The most significant of these is – we cannot assume a T-S adversary to *preserve* its capabilities in the new environment. We are, hence, trying to fit the paremeters in remodeling the adversary to suit our needs.

Till now, we have not been able to do so without significantly reducing the capability of an adversary lower than the threshold of an adversary who at least threatens the system, and well below the capabilities of a powerful attacker.

In summary, this week's work has proven that if we continue in the same direction as before, we will be assuming something nonsensical, like proving security for an adversary who is weak, and not practical at all.