guardtime

Status Report

Intern: Rito

Week 3: 25th May, 2015 to 31st May, 2015

Number of hours worked: 25

Update:

Continuing the previous work on the security proof, we have now reached the following stage. We consider the security game for inverting the function, and in this case, it falls cleanly under the domain of value-domination preserved games, so we can prove that it meets our security requirement. However, it is still to be proven whether considering the information r to be quantum preserves the state in the domain of a ‘linear black box’ as defined in the work of Unhruh et al. In this context, it is important to note that to preserve generality, we will use the proof by Katz and Koo [link] of the original Rompel construction, although it is also true (as noted in the above paper) that some elements are wrong. This particular proof is quite tedious, and in our endeavor to port it towards a quantum setting, we may actually devise a simpler proof as a by-product.

The major issue that I am working on here is that in all these above papers, the hardness or intractability of a problem is not defined at all in most cases, and in the rare occasion where it is defined, the definition only encompasses a classical sense, and that too, in a vague manner. In other words, the existing literature in this particular area is quite confusing and not very helpful. However, I have made some progress in coming up with proper definitions, but I am afraid these in their unscrutinised form may not be suitable.

For obvious reasons, the popular modes of application of the oracle models cannot be used in our case due to entanglement and selective-rewinding. Even in the very useful note by Fang Song, it turns out that there are lots of blank spaces, for example: “When combined with a few other easily verifiable conditions, we can show class-respectful reductions. This in a way justifies a common belief that most post-quantum schemes are indeed quantum- secure, due to some simple form in their classical security reductions which seem “quantum-friendly”.” He then proceeds to state a theorem, without explaining what these apparently “easily verifiable” conditions are. To assume that a scheme is quantum-friendly and proceed accordingly makes a lot of underlying assumptions that we cannot afford.

To sum up, the work that remains to complete the proof is mostly centred around the following elements – finding the correct interpreter, proving linearity in case of quantum *r*, and proving that back-dating as well as existential forgery is unwarranted using the first two. The minor goals that are essential for building the framework include – building the correct definitions (I will be sending these over in a separate file in a couple of days, to check if they match with the requirements.)

Note: Implementation of the architecture makes use of several other phases which are vulnerable to attack in the scenario we are considering (full control of server). In that case, our proof will *not* cover the multi-party computations involved. This may be dealt with in a later stage.