Remarks on RCSP:

1. In the recurring PoR protocol, in section 3.3,

* if the server is (a) honest: then it sends \vv{V\_s}. In this case the contract detects that the client has not provided its input (without requiring the contract to perform any major computation) or (b) malicious: then it sends arbitrary vector. In this case the contract takes all steps of phase 3.g. (including PoRId.Identify()). However, the server automatically pays the contract when it invokes it. Thherefore, y\_S is not needed anymore in this protocol.
* If the client is (a) honest: then it includes in \vv{V\_c} the verifications’ indices in which the server provided no proof or invalid proof. In the former case, the contract can detect that the server has not provided a proof and in the latter case the contract has to take all steps of phase 3.g. (including PoRId.Identify()). So, an honest client has to pay the contract when the server misbehaves. (b) malicious: this is similar to the above case where the server is malicious. In this case, the malicious client pays the contract in advance. Thus, we only need to consider the case where the server is only malicious and make it compensate the client’s cost paid to the contract for the major verification.

1. In recurring PoR protocol, either client or the server needs to call the smart contract to perform the checks after all parties provide their inputs.

* Case one- the server calls the contract: in this case if the server has falsely claimed the client has not provided any inputs, then the contract performs the checks but the server must pay as it has called the contract.
* Case two- the client calls the contract: there are two cases: (a)