SCAPI Project open tasks

This document holds a list of open tasks, when they were open, who has to close them and when they were closed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task name | Task description | Opening date | Owner/Responsible for solving task | Closing date |
| Fix collision resistant hash. | 1)CollisionResistantHash interface should be renamed CryptographicHash  2) TargetCollisionResistant interface will be deleted. Therefore CryptographicHash will become the root of the family  3) Add a new category of SecurityLevel: HashSecLevel<-TargetCollisionResistant<-CollisionResistant  4) All the SHA algorithms implemented in SCAPI are CollisionResistant. | 1/11/11 | Yael |  |
| Review Tapdoor permutation init functions | Check why we need init that accepts public, private key and params for, since in all our implementations we throw exceptions if called. If thought for future use, then specify in SDD | 2/11/11 | Yael |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |