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 |  |
| Add get coordinates functions to dlog GroupElement | 1)Add getPointCoordinates function to ECPoint classes  2)Add getValue function to ZpElement class  3)Add the function getPoint to the ECPoint interface (it is already implemented in the concrete classes) | 2/11/11 | Moriya |  |
| Add the functionality of point at infinity to the ECDlog groups | 1)Add a boolean to ECPoint that indicates if this point is the infinity  2)Add the functionality of the infinity point to the functions that operate the points calculations –multiply, exponentiate, inverse, etc. | 2/11/11 | Moriya |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |