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 | | Category | Task description | Opening date | Owner | Priority | | Closing date |
| Fix collision resistant hash. | Design Issue | | 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 | Design Issue | | 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 | New Feature | | 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 | |  | 6/11/11 |
| Add the functionality of point at infinity to the ECDlog groups | New Feature | | 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 | |  |  |
| Garbled circuits | Future tasks | | This supposedly does "garbled circuits" in Java. We will need to do this after the library is ready (it will probably be one of the first tasks). If we can use their system, this can save us a lot of work. They also put a lot of effort into optimizations…  <http://mightbeevil.org/framework/download.html> | 2/11/11 |  | |  |  |
| Change name of JavaInterface.dll | Design Issue | | Change name to CryptoPPJavaInterface.dll | 2/11/11 | Moriya | |  |  |
| Add getElement() to GroupElements | New Feature | | 1)To ZpElement intfc add BigInteger getElement()  2) To EcElement intfc add some functionality | 2/11/11 | Moriya | |  | 6/11/11 |
| Make getPoint function package private | Design Bug Fix | | And every other function that is only called by the respective Dlog group in the package | 3/11/11 | Moriya | |  | 6/11/11 |
| Rename the Dlog groups we have right now as DlogZpSafePrime and make it inherit from DlogZp and mark it as DDHSecure |  | | In constructor of group check that p = 2q+1 |  |  | |  |  |
| Add to SRS documentation that we need to write a DlogZp that is general |  | |  |  |  | |  |  |
| Add to dloggroupsafeprime a constructor that receives the length of p and chooses a random safe prime p and finds the g |  | |  |  |  | |  |  |
| Bug: ZpGroupParams need to check that p = 2q + 1 and then check primality for both |  | |  |  |  | |  |  |
| In Function createDlogZp  In DlogGroup.cpp of JNI change the name of the argument “element” to “possibleGenerator” |  | |  |  |  | |  |  |
| PointerToGroup is a member variable of CryptoPPDlogZp. It shouldn’t start with capital |  | |  |  |  | |  |  |
| Make all mathematical operations in that don’t involve a specific instance in DlogGroup static. |  | |  |  |  | |  |  |

Possible categories are:

* Bug Fix
* Design Bug Fix
* New Feature
* Design Issue
* Future task

Owner: The person responsible for solving task.

Priority:

* Very Low
* Low
* Regular
* High Priority
* Urgent