Marec Frédéric
KIBEYA Malaika Aisha

TP3 : accréditation anonyme et coloriage de graphe

Description :

Le but de ce troisième TP est de vous faire implémenter une accréditation anonyme par une preuve de connaissance à divulgation nulle de type 3-coloriage de graphe. Plus précisément, on est dans la situation où un utilisateur souhaite convaincre un vérificateur qu'il connaît une manière de colorier entièrement un graphe avec 3 couleurs de telle façon qu'aucun nœud du graphe n'ait la même couleur que l'un des nœuds voisins mais sans révéler aucune autre information à propos de ce coloriage. Voir l'entrée correspondante sous wikipedia pour plus de détails à propos de ce problème: http://fr.wikipedia.org/wiki/Coloration_de_graphe Le TP lui-même se décompose en quatre parties.

Analyse du protocole :

Question 1 :
Pourquoi est ce que si l'utilisateur et le vérificateur sont honnêtes et suivent les directives du protocole, un utilisateur possédant la preuve d'un 3-coloriage pourra toujours convaincre le vérificateur (propriété de *completeness*)?

Le protocole est du type chalenge-response. Si l'utilisateur et le vérificateur sont honnêtes et suivent le protocole le vérificateurs doit toujours accepter la preuve. Car celle-ci correspond a la preuve attendue dans la suivie du protocole défi-réponse.

Question 2 :
Pourquoi est ce qu'un utilisateur qui ne possède pas de preuve d'un 3-coloriage ne pourra pas réussir à convaincre un vérificateur, sauf avec une probabilité négligeable (propriété de *soundness*)?

Si la preuve d'un 3-coloriage est fausse, aucun utilisateur malicieux ne peut convaincre un vérificateur honnête que la preuve est vraie et ceci avec une forte probabilité. Mais il y a toujours une chance négligeable que la preuve d'un 3-coloriage créer au hasard corresponde a celle attendue par le vérificateur. Sinon les preuves sont différente et ne convaincront pas le vérificateur.

Question 3 :
Expliquer en quoi ce protocole est à divulgation nulle (*zero-knowledge* en anglais), c'est à dire qu'il n'apporte aucune autre information au vérificateur que la véracité de l'énoncé.

Le vérificateur n'apprend de la part de l'utilisateur, rien de plus que la véracité de la preuve d'un 3-coloriage, il n'obtient aucune information qu'il ne connaissait déjà sans l'apport de l'utilisateur. Si le vérificateur ne suit pas la procédure, cette définition reste valable aussi longtemps que l'utilisateur suit la procédure. Ce qui définie la propriété *zero-knowledge* d'un protocole chalenge-response.