

Introduction à la cryptologie
TD n° 5 : Preuves à Divulgaration Nulle de Connaissance.

Exercice 1 (Isomorphisme de graphes). On considère des graphes à n sommets. On identifie les sommets à $V = \{1, \dots, n\}$. Deux graphes $G = (V, E)$ and $G' = (V, E')$ sont isomorphes ssi il existe une permutation des sommets qui envoie les arêtes de G sur celles de G' ($E' = \{(\pi(x), \pi(y)) : (x, y) \in E\}$ pour une permutation π).

1. Construire un protocole à divulgation nulle de connaissance par lequel un prouveur prouve à un vérifieur honnête qu'il connaît une permutation π réalisant un isomorphisme entre deux graphes G_0 et G_1 .

Indication. Le prouveur envoie une permutation aléatoire d'un des deux graphes. Le vérifieur pose une question binaire.

2. Dédire un schéma de signature reposant sur l'isomorphisme de graphe.

Exercice 2 (Non-isomorphisme de graphes). Construire un protocole à divulgation nulle de connaissance face à un vérifieur honnête par lequel un prouveur non borné calculatoirement prouve à un vérifieur polynomial que deux graphes G_0 et G_1 ne sont pas isomorphes.

Exercice 3 (Non-résiduosit  quadratique). Construire un protocole à divulgation nulle de connaissance face à un vérifieur honnête par lequel un prouveur qui connaît la factorisation d'un module RSA N prouve à un vérifieur polynomial que $x \in \mathbb{Z}_N^*$ n'est pas un carré modulo N .

Indication : connaissant la factorisation du module RSA N , il est possible de calculer si un entier donné est un carré modulo N en temps polynomial (en utilisant le symbole de Jacobi).

Exercice 4 (Preuve de connaissance d'une représentation). Considérons un groupe \mathbb{G} d'ordre premier q et g et h deux générateurs de \mathbb{G} . Soit $y = g^s h^t$. Proposer une preuve de connaissance du couple (s, t) à divulgation nulle de connaissance face à un vérifieur honnête.

Exercice 5 (Preuve de connaissance d'un logarithme discret). Considérons un groupe \mathbb{G} d'ordre premier q et g un générateur de \mathbb{G} et $y = g^x \in \mathbb{G}$. Considérons le protocole suivant par lequel Alice veut prouver sa connaissance de x .

Engagement : Alice tire uniformément aléatoirement $k \in \mathbb{Z}_q^*$ et calcule $r = g^k \in \mathbb{G}$. Elle envoie r à Bob.

Challenge : Bob répond en envoyant un élément $c \in \mathbb{Z}_q$ tiré uniformément aléatoirement.

Réponse : Alice répond en envoyant $s = k - cx \pmod q$ et Bob accepte si $r = g^s y^c$ dans le groupe \mathbb{G} .

1. Montrer qu'il s'agit d'une preuve de connaissance de x à divulgation nulle de connaissance face à un vérifieur honnête.
2. Décrire le schéma de signature correspondant (signatures de Schnorr).
3. Imaginer un protocole à divulgation nulle de connaissance qui prouve que $(g^a, g^b, g^c) \in \mathbb{G}^3$ appartient au langage Diffie-Hellman (i.e. $c = ab$). **Indication :** on prouve la connaissance du logarithme discret de g^a and base g , et de g^c en base g^b , en prouvant que c'est le même logarithme. Pour ce dernier point, on utilise le même challenge k . La réponse s est la même ssi c'est le logarithme est le même.

Exercice 6 (Un vote électronique simple). Supposons que n personnes votent entre deux candidats, avec le protocole suivant.

- Une autorité de confiance choisit un chiffrement à clef publique, avec une paire clef privée/clef publique ElGamal ($sk = x, pk = g^x$), et publie pk .
 - Chaque votant i choisit son candidat $v_i \in \{0, 1\}$ en chiffrant $g_i^{v_i}$ avec ElGamal, et publie le résultat.
 - Le résultat du vote est le produit des chiffrés (homomorphisme multiplicatif). L'autorité de confiance déchiffre le résultat $g^{v_1 + \dots + v_n}$ et publie une preuve que c'est bien le déchiffrement du produit des chiffrés.
1. Comment récupère-t-on le résultat effectif du vote $v_1 + \dots + v_n$?
 2. Argumenter que la dernière étape doit être correcte, sûre, et à divulgation nulle de connaissance.
 3. Proposer une manière de réaliser cette dernière étape qui assure ces propriétés.

Indication. Voir exercice précédent.