Master CSI 2 2019-2020

Cryptologie Avancée — 4TCY903U

Responsables : G. Castagnos – G. Zémor

Devoir Surveillé — 4 novembre 2019

Documents non autorisés

Partie G. Zémor

– **Exercice 1.** On souhaite réaliser un protocole sans divulgation qui démontre qu'un certain graphe G à n sommets est hamiltonien. Ce graphe est connu de toutes les parties concernées. Les sommets du graphe sont numérotés de 1 à n et il est donné par une matrice d'adjacence.

On propose un protocole où le prouveur commence par s'engager sur une matrice (a_{ij}) de dimension $n \times n$. On pourra considérer que le prouveur confie au vérificateur n^2 enveloppes marquées (i,j), $1 \leq i,j \leq n$, et que (a_{ij}) est censée être une matrice d'adjacence d'un graphe, c'est-à-dire symétrique, telle que $a_{ii} = 0$ et $a_{ij} = 0$ ou 1.

Le vérificateur tire un bit b aléatoire et le révèle au prouveur :

— si $b = 0$ le prouveur révèle une permutation σ de $\{1, 2, \dots, \}$ et autorise le vérificateur à ouvrir toutes les enveloppes.

— si $b = 1$ le prouveur autorise le vérificateur à ouvrir n enveloppes soigneusement choisies.

Terminer la description du protocole. Que doit vérifier le vérificateur dans les deux cas ? Montrer que le protocole est complet, valide et sans divulgation.

– **Exercice 2.** Soient donnés un nombre premier p et deux entiers g et h chacun d'ordre multiplicatif q modulo p, pour q un diviseur premier de $p-1$. Un prouveur souhaite démontrer à un vérificateur qu'un entier Y modulo p est de la forme $Y = g^x h^y$ où y est un entier arbitraire et où $x = 0$ ou $x = 1$.

On propose le protocole suivant.

— Le prouveur choisit u_0, u_1, r des entiers aléatoires uniformes de $\mathbf{Z}/q\mathbf{Z}$, puis il calcule dans $\mathbf{Z}/p\mathbf{Z}$ et communique au vérificateur les quantités

$$a_0 = h^{u_0} g^{-xr}, \quad a_1 = h^{u_1} g^{(1-x)r}.$$

— le vérificateur communique au prouveur le défi $d \in \mathbf{Z}/q\mathbf{Z}$.

— Le prouveur calcule dans $\mathbf{Z}/q\mathbf{Z}$

$$\begin{aligned} e &= x(d-r)+(1-x)r \\ z_0 &= u_0+(d-e)y \\ z_1 &= u_1+ey \end{aligned}$$

puis communique au vérificateur e, z_0, z_1.

— Le vérificateur accepte si

$$\begin{aligned} h^{z_0} &= a_0 Y^{d-e} \\ h^{z_1} &= a_1 (Yg^{-1})^e \end{aligned}$$

(a) Démontrer que le protocole est complet.

(b) Démontrer que le protocole est valide. On pourra montrer en particulier que si un faux prouveur est capable de répondre à deux défis distincts d et d' alors Y est bien de la forme requise. On distinguera le cas où le faux prouveur répond aux deux défis d, d' avec un même e ou bien avec des e et e' distincts.

(c) Démontrer que le protocole est sans divulgation (Zero-knowledge).

Partie G. Castagnos

– **Exercice 3.** Dependent-RSA (Pointcheval 99)

On considère la variante suivante de RSA. Soit k un paramètre de sécurité et un algorithme polynomial probabiliste, GenRSA, qui prend en entrée 1^k et ressort les paramètres n, e, d de RSA. Pour chiffrer $m \in (\mathbf{Z}/n\mathbf{Z})^\times$, on choisit $r \xleftarrow{\$} (\mathbf{Z}/n\mathbf{Z})^\times$ et on calcule $A = r^e, B = m \times (r+1)^e$. Le couple (A, B) est le chiffré pour la clef publique $pk = (n, e)$.

(a) Quelle est la clef privée ? Décrire l'algorithme de déchiffrement.

(b) Ce schéma a-t-il des propriétés homomorphes ?

On fait l'hypothèse suivante (DRSA) : étant donné (n, e) retourné par GenRSA, il est difficile de distinguer des couples d'éléments de la forme $(r^e, (r+1)^e)$ avec r tiré uniformément dans $(\mathbf{Z}/n\mathbf{Z})^\times$ de couples d'éléments tirés uniformément dans $(\mathbf{Z}/n\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times$

(c) Donner une formulation précise de cette hypothèse DRSA sous forme d'expérience.

(d) Montrer que le schéma de chiffrement est $\mathsf{IND-CPA}$ sous l'hypothèse DRSA.

– **Exercice 4.** Soit G un groupe cyclique d'ordre premier q et soit g un générateur de G. Dans ce qui suit, on suppose G, q, g fixés.

(a) Soit X, Y deux éléments de G et a, b deux éléments de $\mathbf{Z}/q\mathbf{Z}$. Soit $Z' \in G$ une solution du problème calculatoire Diffie-Hellman, CDH, sous l'entrée (Xg^a, Yg^b), c'est à dire tel que (Xg^a, Yg^b, Z') soit un triplet Diffie-Hellman. Montrer que connaissant a, b et Z' il est possible de calculer en temps polynomial une solution du problème CDH sous l'entrée (X, Y).

(b) Soit $\mathcal{A}$ un algorithme polynomial probabiliste ayant un succès $1/100$ pour résoudre le problème CDH dans le groupe G. À l'aide de la question précédente, construire un algorithme polynomial probabiliste $\mathcal{B}$ utilisant $\mathcal{A}$, ayant un succès supérieur à $1 - e^{-5} \approx 0,99$ pour retourner une liste d'éléments de G contenant une solution d'un problème CDH. Pour l'analyse de la probabilité de succès, on pourra utiliser le fait que pour tout réel z, $1 - z \leqslant e^{-z}$.