Master CSI 2 2020-2021

Cryptologie Avancée — 4TCY903U

Responsables : G. Castagnos – G. Zémor

Devoir Surveillé — 19 octobre 2020

Documents non autorisés

Partie G. Zémor

– **Exercice 1.** On rappelle que le problème de décision SAT prend en entrée une formule booléenne sur n variables $x_1, x_2, \dots x_n$,

$$f = C_1 \wedge C_2 \wedge \cdots \wedge C_k$$

où chaque clause C_i est le $\vee$ d'un certain ensemble de littéraux (une variable ou sa négation). Le problème consiste à décider si la formule f est ou non satisfaisable, i.e. s'il existe une instantiation des variables binaires x_i telle que $f = 1$. Montrer que si on dispose d'un algorithme en temps polynomial qui résout le problème de décision SAT, alors il existe un algorithme polynomial qui *calcule* une valeur du n-uple $(x_1, \dots, x_n)$ qui satisfait f.

– **Exercice 2.** Soient g et h deux entiers modulo p, tous les deux d'ordre multiplicatif q, où q est un diviseur premier de $p-1$. Soient x et y deux autres entiers modulo p. On propose le protocole suivant, dont le but est de montrer qu'il existe un $s \bmod q$ tel qu'on ait simultanément $g^s = x \bmod p$ et $h^s = y \bmod p$.

- Le prouveur émet deux entiers a et b modulo p,
- Le vérificateur émet un entier c modulo q,
- Le prouveur émet un entier z et le prouveur vérifie que $g^z = ax^c$ et $h^z = by^c$ modulo p.

Montrer que le protocole est bien complet, valide et sans divulgation. Quelle est la probabilité qu'un faux prouveur ne soit pas démasqué dans le cas où il n'est pas vrai que l'entier s prétendu existe ?

– **Exercice 3.** Soit G un graphe à n sommets. Une *k-clique* du graphe est un sous-ensemble de k sommets du graphe dont tous les k sommets sont deux à deux adjacents. On se propose de démontrer, sans divulgation, que le graphe G contient un stable à k sommets.

Le protocole consiste pour le prouveur à choisir une permutation aléatoire ϕ des sommets du graphe, puis à s'engager sur une matrice d'adjacence A_{ij} du graphe permuté, où $A_{ij} = 1$ si le sommet i est adjacent au sommet j et $A_{ij} = 0$ sinon. S'engager sur la valeur A_{ij} consiste à la placer dans une enveloppe, qui peut être matérialisée par une fonction cryptographique, et la confier au vérificateur. Le vérificateur renvoie un défi ε qui vaut 0 ou 1.

(a) Dans le cas $\varepsilon = 0$, le prouveur autorise l'ouverture de toutes les enveloppes. Que révèle-t-il en plus ? Que vérifie le vérificateur ?

(b) Dans le cas $\varepsilon = 1$, quelles sont les enveloppes dont le prouveur autorise l'ouverture ? Que vérifie le vérificateur ?

(c) Détailler la complétude et la validité. Quelle est la probabilité pour le prouveur de répondre comme prévu au défi s'il n'est pas vrai que le graphe G contient une k-clique ?

(d) Pourquoi le protocole est-il sans divulgation ?

Partie G. Castagnos

– **Exercice 4.** On définit un protocole d'échange de clef $\mathcal{P}$ entre Alice et Bob à deux passes et sa sécurité. Soit k un paramètre de sécurité, on suppose connu par tous un groupe cyclique G, son ordre q avec $|q| = k$, et un générateur g. On suppose que toutes les quantités échangées et la clef secrète établie sont des éléments de G. Le protocole se déroule ainsi :

1. Bob à partir de G, q, g produit un état s_B et un élément $X \in G$. Il envoie X à Alice ;
2. Alice à partir de G, q, g produit un état s_A et un élément $Y \in G$. Elle envoie Y à Bob ;
3. Alice calcule à partir de s_A et X une clef $K_A \in G$. De même Bob calcule à partir de s_B et Y une clef $K_B \in G$.

Le protocole $\mathcal{P}$ est correct si $K_A = K_B =: K$. De plus, il est sûr si un adversaire $\mathcal{A}$ observant les données échangées par Alice et Bob ne peut distinguer la clef K établie d'un élément de G aléatoire. Plus formellement on définit $\mathbf{Exp}_{\mathcal{P},k}(\mathcal{A})$:

1. Sous l'entrée 1^k Alice et Bob exécutent le protocole $\mathcal{P}$. Ceci produit les quantités échangées X et Y et la clef K éléments de G d'ordre q avec $|q| = k$;
2. on choisit un bit aléatoire $b^\star \xleftarrow{\$} \{0,1\}$. Si $b^\star = 1$ alors $Z := K$ sinon Z est tiré uniformément dans G ;
3. on donne (G, q, g, X, Y, Z) à $\mathcal{A}$ qui sort un bit b ;
4. la sortie de l'expérience est 1 si $b = b^\star$ et 0 sinon.

Le protocole $\mathcal{P}$ est sûr si pour tout algorithme polynomial probabiliste $\mathcal{A}$, l'avantage de $\mathcal{A}$, défini par $\mathbf{Adv}_{\mathcal{P},k}(\mathcal{A}) = \left|\Pr(\mathbf{Exp}_{\mathcal{P},k}(\mathcal{A}) = 1) - \frac{1}{2}\right|$, est négligeable.

(a) Que sont $s_B, s_A, X, Y, K_A, K_B, K$ dans le cas du protocole de Diffie-Hellman ? Quelle est l'hypothèse qui assure que le protocole est sûr ?

(b) Montrer qu'à partir de n'importe quel protocole d'échange de clef $\mathcal{P}$ à deux passes correct, on peut construire un schéma de chiffrement à clef publique Π. Montrer que si $\mathcal{P}$ est sûr alors Π est sémantiquement sûr pour des attaques à clairs choisis.

– **Exercice 5.** On considère l'hypothèse DDH dans le cas où le groupe cyclique utilisé est $G := (\mathbf{Z}/p\mathbf{Z})^\times$ où p est un nombre premier impair. On considère donc Gen un algorithme polynomial qui prend en entrée 1^k et retourne un nombre premier p avec $|p| = k$ et un générateur g de $G := (\mathbf{Z}/p\mathbf{Z})^\times$.

On rappelle que le symbole de Legendre $\left(\frac{x}{p}\right)$ d'un élément x de $(\mathbf{Z}/p\mathbf{Z})^\times$ vaut 1 si x est un carré modulo p et -1 si ce n'est pas un carré.

(a) Que vaut $\left(\frac{g}{p}\right)$?

(b) Soient x, y deux éléments de $\mathbf{Z}/(p-1)\mathbf{Z}$, et $X := g^x$ et $Y := g^y$. Montrer comment à partir de X et Y on peut calculer le symbole $\left(\frac{g^{xy}}{p}\right)$.

(c) En déduire que l'hypothèse DDH est fausse pour $G = (\mathbf{Z}/p\mathbf{Z})^\times$. Pour cela décrire un algorithme $\mathcal{D}$ attaquant le problème sous-jacent et montrer que son avantage est non négligeable.

(d) Détailler comment l'algorithme $\mathcal{D}$ construit précédemment peut donner une attaque sur le chiffrement ElGamal défini dans le groupe tout entier $G := (\mathbf{Z}/p\mathbf{Z})^\times$. Comment peut on s'en protéger ?