Master CSI 2 2011-2012

Cryptologie Avancée — M1MA9W07

Responsables : G. Castagnos – G. Zémor

Devoir surveillé — 7 novembre 2011

Durée 1h30 — Documents non autorisés
Rédiger les deux parties sur des copies séparées

Partie G. Zémor

1 Décision et calcul

Montrer que si P=NP alors il existe un algorithme polynomial qui prend en entrée une formule booléenne $f(x_1, \ldots, x_n) = C_1 \wedge \ldots \wedge C_k$ et qui

1. dit si la formule est satisfaisable,
2. et dans ce dernier cas, *calcule* et exhibe un n-uple $(a_1, \ldots, a_n) \in \{0,1\}^n$ qui satisfait f, i.e. tel que $f(a_1, \ldots, a_n) = 1$.

2 P vs NP

Soit $\Lambda \subset \Sigma^*$ un langage NP-complet. Soit $\overline{\Lambda} = \{x \in \Sigma^* \mid x \notin \Lambda\}$. Montrer que si $\overline{\Lambda} \in$ P, alors P = NP.

3 Cliques

On rappelle qu'une clique de taille k dans un graphe est un sous-graphe à k sommets deux à deux reliés par une arête (un sous-graphe complet). On rappelle que le problème de décision CLIQUE est donné par :

I : un graphe G, un entier k
Q : le graphe G contient-il une clique à k sommets ?

On rappelle enfin que le problème CLIQUE est NP-complet. On considère maintenant le problème de décision CLIQUE-$n/2$:

I : un graphe G à n sommets où n est pair
Q : le graphe G contient-il une clique à $n/2$ sommets ?

(a) CLIQUE-$n/2$ est-il dans NP ?

(b) Exhiber une réduction polynomiale de CLIQUE-$n/2$ vers CLIQUE.

(c) Exhiber une réduction polynomiale de CLIQUE vers CLIQUE-$n/2$. On pourra traiter séparément les deux cas, $k > n/2$ et $k < n/2$, en agrandissant de manière appropriée le graphe de départ.

(d) CLIQUE-$n/2$ est-il NP-complet ?

4 Satisfaisabilité

Soit f une formule booléenne sous la forme $f = C_1 \wedge \ldots \wedge C_k$ où dans chaque clause C_i n'interviennent que l'opérateur $\vee$. On dira qu'une clause $C_i = y_1 \vee y_2 \vee y_3$ est $\neq$-*satisfaite* par un choix des variables y_i si C_i est satisfaite mais l'on n'a pas simultanément $y_1 = 1$, $y_2 = 1$, $y_3 = 1$.

(a) Soit $\neq$SAT le problème :

I : Une formule booléenne $f = C_1 \wedge \ldots \wedge C_k$

Q : la formule f est-elle $\neq$-satisfaisable ?

Montrer que $\neq$SAT est dans NP. Existe-t-il une réduction polynomiale de $\neq$-SAT vers SAT ?

(b) Montrer que l'on obtient une réduction polynômiale de 3-SAT vers $\neq$-SAT en remplaçant chaque clause $C_i = y_1 \vee y_2 \vee y_3$ par la sous-formule

$$(y_1 \vee y_2 \vee z_i) \wedge (\overline{z}_i \vee y_3 \vee b)$$

où z_i est une variable auxiliaire associée à la clause C_i, et où b est une variable supplémentaire unique.

(c) En déduire que le problème $\neq$SAT est NP-complet.

Partie G. Castagnos

5 Une attaque sur ElGamal

(a) Donner la définition précise (bien détailler les 3 algorithmes) du système de chiffrement ElGamal dans le cas où le groupe cyclique utilisé est $G := (\mathbf{Z}/p\mathbf{Z})^\times$ où p est un nombre premier impair. On suppose que l'ensemble des messages clairs est G tout entier.

(b) Rappeler la définition précise de l'hypothèse garantissant la sécurité $\mathsf{IND} - \mathsf{CPA}$ de ElGamal toujours dans le cas $G := (\mathbf{Z}/p\mathbf{Z})^\times$.

(c) 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. On note dans la suite g un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$. Que vaut $\left(\frac{g}{p}\right)$?

(d) 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 $\left(\frac{g^{xy}}{p}\right)$.

(e) En déduire que l'hypothèse énoncée en (b) 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.

(f) Détailler comment l'algorithme $\mathcal{D}$ construit précédemment peut donner une attaque sur ElGamal. Comment peut on s'en protéger ?