Master CSI 2 2016-1017

Cryptologie Avancée — 4TCY903U

Responsables : G. Castagnos – G. Zémor

Examen — 5 janvier 2017

Durée 3h — Documents non autorisés

Partie G. Castagnos

– **Exercice 1.** Soit $\Pi = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ un schéma de chiffrement asymétrique. On note $\mathcal{M}$ l'espace des messages clairs pour Π. Soit $\mathcal{A}$ un algorithme attaquant Π et k un paramètre de sécurité. Soit $n > 0$, un entier. On définit l'expérience $n-\mathsf{IND}-\mathsf{CPA}$, $\mathbf{Exp}_{\Pi,k}^{n-\mathsf{IND}-\mathsf{CPA}}(\mathcal{A})$ comme suit :

1. On lance l'algorithme $\mathsf{KeyGen}(1^k)$ pour obtenir les clefs (pk, sk)
2. On choisit un bit aléatoire avec équiprobabilité $b^\star \xleftarrow{\$} \{0,1\}$
3. On donne pk à $\mathcal{A}$. Au cours de son exécution, $\mathcal{A}$ émet n couples de messages clairs : pour $i = 1, \ldots, n$, quand $\mathcal{A}$ émet $(m_{i,0}, m_{i,1}) \in \mathcal{M} \times \mathcal{M}$, on lui donne $c_i^\star$, un chiffré de $m_{i,b^\star}$: $c_i^\star \leftarrow \mathsf{Encrypt}(pk, m_{i,b^\star})$
4. À la fin de son exécution, $\mathcal{A}$ retourne un bit b
5. La sortie de l'expérience est 1 si $b = b^\star$ et 0 sinon.

L'avantage de l'attaquant $\mathcal{A}$ est défini par

$$\mathbf{Adv}_{\Pi,k}^{n-\mathsf{IND}-\mathsf{CPA}}(\mathcal{A}) = \left| \Pr\left(\mathbf{Exp}_{\Pi,k}^{n-\mathsf{IND}-\mathsf{CPA}}(\mathcal{A}) = 1 \right) - \frac{1}{2} \right|.$$

Le schéma Π est dit sûr au sens $n-\mathsf{IND}-\mathsf{CPA}$ si pour tout algorithme polynomial probabiliste $\mathcal{A}$ cet avantage est négligeable.

(a) À quelle notion de sécurité correspond le cas $n = 1$?

(b) Soit $n > 1$ un entier. À partir du schéma Π, on construit un schéma $\Pi' = (\mathsf{KeyGen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$. L'algorithme de génération de clefs est inchangé : $\mathsf{KeyGen}' := \mathsf{KeyGen}$. L'algorithme de chiffrement $\mathsf{Encrypt}'$ est défini comme suit. L'espace des messages clairs est inchangé : $\mathcal{M}' = \mathcal{M}'$. Soit $m \in \mathcal{M}$ à chiffrer. On tire un bit b tel que $b = 0$ avec probabilité $1/n$ et $b = 1$ avec probabilité $1 - 1/n$. Si $b = 0$, le chiffré est $c := (c_1, c_2) := (m, 0)$. Si $b = 1$, le chiffré est $c := (c_1, c_2) := (\mathsf{Encrypt}(pk, m), 1)$. L'algorithme de déchiffrement $\mathsf{Decrypt}'$ sous l'entrée (c_1, c_2) retourne c_1 si $c_2 = 0$ et $\mathsf{Decrypt}(sk, c_1)$ si $c_2 = 1$.

Montrer qu'il existe un attaquant polynomial probabiliste $\mathcal{A}$ attaquant Π' tel que

$$\mathbf{Adv}_{\Pi',k}^{n-\mathsf{IND}-\mathsf{CPA}}(\mathcal{A}) \geqslant (1 - e^{-1})/2 \approx 0,3$$

On pourra utiliser le fait que pour tout réel z, $1 - z \leqslant e^{-z}$.

(c) Soit $n > 1$ un entier. Soit $\mathcal{A}$ un attaquant polynomial probabiliste contre la notion $n-\mathsf{IND}-\mathsf{CPA}$ pour le schéma Π. Construire à partir de $\mathcal{A}$ un algorithme polynomial probabiliste $\mathcal{B} = (\mathcal{B}_1, \mathcal{B}_2)$ attaquant la notion $\mathsf{IND}-\mathsf{CPA}$ pour le schéma Π tel que

$$\mathbf{Adv}^{\mathsf{IND}-\mathsf{CPA}}_{\Pi,k}(\mathcal{B}) = \frac{1}{n}\mathbf{Adv}^{n-\mathsf{IND}-\mathsf{CPA}}_{\Pi,k}(\mathcal{A}).$$

Conclure. **Indication** : $\mathcal{B}_1$ pourra choisir aléatoirement en début d'exécution le nombre de fois ℓ où il chiffre le premier élément d'un couple choisi par $\mathcal{A}$, puis lors du calculs des probabilités, on pourra décomposer suivant la valeur de ℓ.

(d) Soit GenDH un algorithme polynomial qui prend en entrée 1^k et retourne la description d'un groupe cyclique G son ordre q premier tel que $|q| = k$ et un générateur g. Soit $T \in G^3$ un triplet d'éléments de G. On rappelle que T est un triplet DH si $T = (g^x, g^y, g^{xy})$ avec $x, y \in \mathbf{Z}/q\mathbf{Z}$ uniformément distribués et indépendants. Si $T = (g^x, g^y, g^z)$ avec $x, y, z \in \mathbf{Z}/q\mathbf{Z}$ uniformément distribués et indépendants, on dit que T est un triplet aléatoire. On rappelle que le problème DDH consiste à distinguer les triplets DH et les triplets aléatoires.

Donner un algorithme polynomial $\mathcal{R}$ qui prend en entrée $T = (X, Y, Z) \in G^3$ et qui retourne un couple (Y', Z') d'éléments de G tel que $T' := (X, Y', Z') \neq T$ et tel que si T est un triplet DH alors T' est un triplet DH et si T est un triplet aléatoire alors T' est un triplet aléatoire.

(e) On rappelle le fonctionnement du chiffrement Elgamal. L'algorithme KeyGen appelle GenDH puis choisit x aléatoire avec probabilité uniforme dans $\mathbf{Z}/q\mathbf{Z}$ et calcule $X = g^x$. KeyGen retourne $pk = (G, q, g, X)$ et $sk = (G, q, g, x)$. L'algorithme $\mathsf{Encrypt}$ sur l'entrée (pk, m) avec $m \in G$ choisit y uniformément dans $\mathbf{Z}/q\mathbf{Z}$ calcule $Y = g^y$ et $Z = X^y$ dans G et retourne $c = (Y, mZ)$.

Soit $n > 1$ un entier. Soit $\mathcal{A}$ un attaquant polynomial probabiliste contre la notion $n-\mathsf{IND}-\mathsf{CPA}$ pour Elgamal. En utilisant l'algorithme $\mathcal{R}$ de la question précédente, construire à partir de $\mathcal{A}$ un algorithme polynomial probabiliste $\mathcal{D}$ résolvant le problème Diffie-Hellman décisionnel (DDH) tel que

$$\mathbf{Adv}^{\mathsf{DDH}}_{\mathsf{GenDH},k}(\mathcal{D}) = \frac{1}{2}\mathbf{Adv}^{n-\mathsf{IND}-\mathsf{CPA}}_{\mathsf{Elgamal},k}(\mathcal{A}).$$

Conclure.

– **Exercice 2.** Soit k un entier et $\Pi = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ un schéma de chiffrement asymétrique. On suppose que l'espace des messages clairs est $\mathcal{M} := \{0,1\}^{2k}$. On suppose de plus que le chiffrement d'un message $m \in \mathcal{M}$ avec la clef publique pk consiste à prendre $r \in \{0,1\}^k$ avec distribution uniforme puis poser $c = E_{pk}(m, r)$ où E_{pk} est une fonction de $\{0,1\}^{2k} \times \{0,1\}^k$ à valeurs dans l'espace des chiffrés.

Soit $\mathcal{H} : \{0,1\}^{2k} \to \{0,1\}^k$ un oracle aléatoire. À partir de Π, on construit un nouveau schéma de chiffrement $\Pi' = (\mathsf{KeyGen}', \mathsf{Encrypt}', \mathsf{Decrypt}')$ dans le modèle de l'oracle aléatoire. L'algorithme de génération de clefs est inchangé : $\mathsf{KeyGen}' := \mathsf{KeyGen}$. L'algorithme de chiffrement $\mathsf{Encrypt}'$ est défini comme suit. L'espace des messages clairs est $\mathcal{M}' := \{0,1\}^k$. Soit

$m \in \{0,1\}^k$ à chiffrer avec la clef publique pk. On tire $t \in \{0,1\}^k$ avec probabilité uniforme et on pose $c = E_{pk}(m||t, \mathcal{H}(m||t))$ où $||$ désigne la concaténation des chaînes de bits.

(a) Donner la description d'un l'algorithme de déchiffrement $\mathsf{Decrypt}'$ pour Π' qui vérifie que le chiffré est bien formé avant de retourner le message clair.

Dans la suite on note $\mathcal{A}' = (\mathcal{A}'_1, \mathcal{A}'_2)$ un attaquant polynomial probabiliste contre la notion de sécurité $\mathsf{IND-CPA}$ du schéma Π' dans le modèle de l'oracle aléatoire. À partir de $\mathcal{A}'$, on construit $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ un attaquant contre la notion de sécurité $\mathsf{IND-CPA}$ du schéma Π comme suit.

$\underline{\mathcal{A}_1(pk)}$

1. $(m_0, m_1, s) \leftarrow \mathcal{A}'_1(pk)$
2. $t_0, t_1 \xleftarrow{\$} \{0,1\}^k$
3. Retourne $(m_0||t_0, m_1||t_1, s)$

$\underline{\mathcal{A}_2(c^\star, s)}$

1. $b' \leftarrow \mathcal{A}'_2(c^\star, s)$
2. Retourne b'

On note $b^\star$ le bit choisi lors de l'expérience $\mathsf{IND-CPA}$ que joue $\mathcal{A}$. Soit E l'événement « $\mathcal{A}'_2$ demande $(m_{b^\star}, t_{b^\star})$ à son oracle aléatoire » et F l'événement « $\mathcal{A}'_2$ demande $(m_{\bar{b}^\star}, t_{\bar{b}^\star})$ à son oracle aléatoire ».

(b) Compléter la description de $\mathcal{A}$ pour répondre aux requêtes faites par $\mathcal{A}'$ à son oracle aléatoire. De plus comment $\mathcal{A}$ peut il utiliser ces requêtes pour résoudre l'expérience $\mathsf{IND-CPA}$ avec un meilleur avantage ?

(c) Que valent les probabilités suivantes $\Pr(\mathbf{Exp}^{\mathsf{IND-CPA}}_{\Pi,k}(\mathcal{A}) = 1|E)$, $\Pr(\mathbf{Exp}^{\mathsf{IND-CPA}}_{\Pi,k}(\mathcal{A}) = 1|(\bar{E} \text{ et } F))$ et $\Pr(\mathbf{Exp}^{\mathsf{IND-CPA}}_{\Pi,k}(\mathcal{A}) = 1|(\bar{E} \text{ et } \bar{F}))$?

(d) En déduire que

$$\Pr(\mathbf{Exp}^{\mathsf{IND-CPA}}_{\Pi,k}(\mathcal{A}) = 1) - \Pr(\mathbf{Exp}^{\mathsf{IND-CPA}}_{\Pi',k}(\mathcal{A}') = 1) \geqslant -\Pr(\bar{E} \text{ et } F).$$

Conclure.

(e) Adapter ce qui précède pour montrer que Π' est $\mathsf{IND-CCA2}$ dans le modèle de l'oracle aléatoire si Π est $\mathsf{IND-CPA}$.

Partie G. Zémor