Il est important de passer 1h sur la partie asymétrique (I et II) et 1h sur la partie symétrique (III).

I Advanced encryption

Toutes les questions de cette partie sont indépendantes.

On rappelle que le problème DDH consiste, étant donné (g, g^x, g^y, g^z), pour un générateur g d'un groupe $\mathbb{G}$ d'ordre p, à décider si $z = xy$ ou si z est un nombre aléatoire modulo p.

On introduit également le problème DLIN qui consiste, étant donné (u, v, w, u^a, v^b, w^c), pour des générateurs u, v, w de $\mathbb{G}$, à décider si $c = a + b$ ou si c est un nombre aléatoire modulo p.

Soit h un générateur d'un groupe $\mathbb{G}$ d'ordre p premier. On définit un protocole de chiffrement comme suit.

- $sk = \{x, y\}$
- $pk = \{h, u, v\}$ où $u = h^{1/x}$ et $v = h^{1/y}$
- Encrypt(pk, m): choisir deux entiers aléatoires a et b. Retourner $C = (u^a, v^b, m \times h^{a+b})$.

▶ **Question 1.** *Décrire l'algorithme de déchiffrement correspondant à ce protocole.*

▶ **Question 2.** *Ce protocole de chiffrement est-il homomorphe?*

▶ **Question 3.** *Prouver que ce protocole de chiffrement est IND-CPA sûr sous l'hypothèse DLIN.*

▶ **Question 4.** *Ce protocole satisfait-il la propriété IND-CCA sous la même hypothèse?*

▶ **Question 5.** *Soit $\mathcal{A}$ un algorithme capable de résoudre le problème DLIN. Montrer que $\mathcal{A}$ peut être utilisé pour résoudre le problème DDH pour n'importe quelle instance (g, g^x, g^y, g^z). En d'autres termes, construire $\mathcal{B}$ un adversaire contre DDH s'appuyant sur $\mathcal{A}$. Quel est son avantage ?"*

II Zero-Knowledge

On rappelle qu'un couplage est une application bilinéaire $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, c'est-à-dire que $\forall\ g \in \mathbb{G}_1$, $h \in \mathbb{G}_2$ et entiers a et b, on a

$$e(g^a, h^b) = e(g, h)^{a \times b}.$$

Soit p l'ordre de ces groupes.

On rappelle également que le schéma de signature Boneh-Boyen utilise une clé secrète x et une clé publique comprenant $g \in \mathbb{G}_1$ et $(h, h_1 = h^x) \in \mathbb{G}_2$. Une signature S sur un message m est $g^{\frac{1}{x+m}}$. L'équation de vérification est alors:

$$e(S, h_1 \times h^m) = e(g, h)$$

.

▶ **Question 1.** *Soit S une signature Boneh-Boyen sur un message m. On suppose S publique et m secret. Montrer que le protocole de la Figure 1 est une preuve de connaissance zero-knowledge du message m pour lequel S est une signature valide.*

▶ **Question 2.** *Soient g_1 et g_2 deux clés publiques El Gamal. On peut construire le double chiffrement de S de la manière suivante: 1) sélectionner r aléatoire et 2) calculer $C = (c_1, c_2, c_3)$ où $c_1 = g^r, c_2 = g_1^r \times S, c_3 = g_2^r \times S$. Ecrire un protocole de preuve zéro-knowledge qu'un tel chiffré est bien formé. Concrètement, cela signifie qu'il faut prouver connaissance de r et que le message dissimulé par g_1^r dans c_2 et g_2^r dans c_3 est le même.*

$$\begin{array}{lcr}
\text{Prouveur} & & \text{Vérificateur} \\
\hline
k \text{ entier modulo } p & & \\
 & \xrightarrow{K = e(S,h)^k} & \\
 & \xleftarrow{c} & c \text{ entier aléatoire modulo } p \\
z = k + c * m & \xrightarrow{z} & e(S,h)^z \stackrel{?}{=} K * [e(g,h) \times e(S,h_1)^{-1}]^c \\
\hline
\end{array}$$

Figure 1: Preuve de connaissance de message

III Chiffrement symétrique

▶ **Question 1.** *Questions de cours:*

1. *Qu'est-ce qu'une PRF (Pseudo-Random Functions) ?*
2. *Rappeler le jeu de sécurité d'une PRF et définir l'avantage de l'adversaire.*
3. *Est-ce qu'un schéma de chiffrement par bloc est une PRF ? Si oui, quel est l'avantage ?*
4. *Comment transformer un schéma de chiffrement par bloc en PRF avec un avantage plus petit ?*

On dira qu'une famille de fonctions $\{F : \mathcal{K} \times \mathcal{M} \leftarrow \mathcal{C}\}$ est un cipher si c'est un schéma de chiffrement déterministe. Pour chaque K, F_K est une injection entre $\mathcal{M}$ et $\mathcal{C}$ et F_K^{-1} existe. Un schéma de chiffrement par bloc, comme AES, est un cipher avec $\mathcal{M} = \mathcal{C} = \{0,1\}^n$.

On dit qu'un schéma atteint la notion de sécurité appelée privacy si l'avantage

$$\Pr[K \leftarrow \mathcal{K} : A^{E_K()} = 1] - \Pr[K \leftarrow \mathcal{K} : A^{E_K(\$^{|\cdot|})} = 1],$$

est négligeable, où l'oracle $\$^{|\cdot|}$ retourne une chaîne aléatoire de même longueur le message chiffré. La notation A^O signifie que A fait appel à l'oracle O.

▶ **Question 2.** *Représenter graphiquement le jeu de sécurité entre un challenger et l'adversaire. Expliquer ce que veut dire intuitivement cette notion.*

★ **Question 3.** *Montrer que la notion privacy est équivalente à la notion sécurité IND-CPA. (On donnera une réduction entre ces deux notions dans les 2 sens.)*

On veut faire un schéma de chiffrement avec un cipher.

▶ **Question 4.** *Pourquoi un cipher n'atteint pas la notion privacy ? (Donner un adversaire et calculer son avantage.)*

Pour atteindre la notion de privacy avec un cipher, on va utiliser un encodage. On appelle schéma d'encodage de l'espace $\mathcal{M}$ vers $\mathcal{M}^*$ une paire d'algorithmes $(Encode, Decode)$. L'algorithme $Encode$ peut être randomisé: pour encoder $M \in \mathcal{M}$, il génère un random r et $M^* = Encode(M, r) \in \mathcal{M}^*$. Pour tout message M et random r, on a $|\mathsf{Encode}(M, r)| = \ell(|M|)$ où $|M|$ représente la taille en bits de M et ℓ une fonction longueur. L'algorithme $Decode$ prend en entrée $M \in \{0,1\}^*$, et retourne $M \in \mathcal{M}$ ou $\perp$. Si $Decode(M^*)$ est une chaîne binaire, on dit que M^* est *valide*. On veut que pour tout message $M \in \mathcal{M}$, et tout random r, $Decode(Encode(M, r)) = M$.

On dit que le schéma d'encodage est ϵ-colliding si pour tout entier q et tout adversaire A qui fait au plus q requêtes, la probabilité que deux de ces requêtes reçoivent la même réponse valide est au plus $\epsilon(q)$:

$$\Pr[(M_1^*, \ldots, M_q^*) \leftarrow \mathsf{Responses}A^{Encode(\cdot)} : i < j \text{ s.t. } M_i^* \neq \perp, M_j^* \neq \perp, \text{ and } M_i^* = M_j^*] \leq \epsilon(q).$$

On dit que $(M_1^*, \ldots, M_q^*)$ collisionne s'il existe deux messages différents de $\perp$ qui sont égaux.

▶ **Question 5.** *Montrer que l'encodage qui ajoute un bloc aléaoire de 128 bits en tête du message est un schéma d'encodage avec quelle fonction ϵ ?*

▶ **Question 6.** *Si comme encodage, on ajoute un compteur sur 128 bits au début du message. Quelle est la fonction ϵ ?*

Soit $\mathsf{Encode} = (Encode, Decode)$ un schéma d'encodage de $\mathcal{M}$ vers $\mathcal{M}^*$ et soit $F = \{F_K : \mathcal{M}^* \to \mathcal{M}^*\}$ un chiffrement avec comme espace de clé $\mathcal{K}$. Alors le schéma d'encapsulation $F \circ \mathsf{Encode} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$:

(*i*) $\mathcal{K}$ choisit une clé aléatoire $K \leftarrow \mathcal{K}$ et la retourne.

(*ii*) $\mathcal{E}_K(M)$ calcule $M^* \leftarrow Encode(M)$, retourne $\perp$ si $M^* = \perp$, et sinon $C \leftarrow F_K(M^*)$ et le retourne.

(*iii*) $\mathcal{D}_K(C)$ retourne $\perp$ si $C \notin \mathcal{M}^*$ et sinon calcule $M^* \leftarrow F_K^{-1}(C)$ et $M \leftarrow Decode(M^*)$, et retourne M.

On veut montrer le théorème suivant:

Theorem 1. *Soit* $\mathsf{Encode} = (Encode, Decode)$ *un schéma d'encodage ϵ-colliding de $\mathcal{M}$ vers $\mathcal{M}^*$ et* $F = \{F_K : \mathcal{M}^* \to \mathcal{M}^*\}$ *un chiffrement avec espace de clé $\mathcal{K}$. Alors* $\mathbf{Adv}^{\mathrm{priv}}_{F\circ\mathsf{Encode}}(t, q, \mu) \leq \mathbf{Adv}^{\mathrm{prf}}_F(t', q, \mu) + \epsilon(q)$*, avec $t' = t + O(\mu)$. (t représente le temps de l'algorithme contre la privacy, q le nombre de requêtes de chiffrement et μ la taille en bits de tous les messages).*

▶ **Question 7.** *Pourquoi l'adversaire de la question 4 ne fonctionne pas dans ce cas avec les deux encodages définis précédemment ?*

Pour montrer ce théorème, on va utiliser plusieurs étapes et définir plusieurs adversaires. Soit B l'adversaire attaquant la privacy de $F \circ \mathsf{Encode}$ en temps t, q requêtes totalisant une longueur de message au plus μ. Pour borner l'avantage de B, on introduit les algorithmes suivants.

L'algorithme D est un distingueur pour F. Il a accès à un oracle pour une permutation aléatoire tirée parmis toutes les permutations sur $\mathcal{M}^*$. Ce distingueur peut utiliser l'attaquand B.

L'algorithme A est un adversaire contre la collision du schéma d'encodage. Le challengeur est un oracle Encode. Il choisit une permutation f aléatoire sur $\mathcal{M}^*$ au hasard (ou la simule). Il exécute B. Quand B fait une requête M, l'algorithme A calcule $M^* \leftarrow Encode(M)$ et $C \leftarrow f(M^*)$. Il retourne C à B. Quand B termine, A aussi.

On définit les probabilités suivantes:

$$
\begin{aligned}
p_1 &= \Pr[K \leftarrow \mathcal{K} : B^{E_K(\cdot)} = 1] && (1)\\
p_2 &= \Pr[K \leftarrow \mathcal{K} : B^{E_K(\$^{|\cdot|})} = 1] && (2)\\
p_3 &= \Pr[K \leftarrow \mathcal{K} : D^{E_K(\cdot)} = 1] && (3)\\
p_4 &= \Pr[\pi \leftarrow \mathbf{Perm}(\mathcal{M}^*) : D^{\pi(\cdot)} = 1] && (4)\\
p_5 &= \Pr[(M_1^*, \ldots, M_q^*) \leftarrow \mathsf{Responses}A^{Encode(\cdot)} : i < j \text{ s.t. } M_i^* \neq \perp, M_j^* \neq \perp, \text{ and } M_i^* = M_j^*] && (5)
\end{aligned}
$$

▶ **Question 8.** *Montrer que:*

1. $p_1 = p_2$ *et* $p_2 \geq p_4 - p_5$
2. $\mathbf{Adv}^{\mathrm{priv}}_{F\circ\mathsf{Encode}}(B) \leq \mathbf{Adv}^{\mathrm{prp}}_F(D) + \epsilon(q)$