6. Dependent-RSA

6.1 Chiffrement RSA de base

Considérons le schéma de chiffrement suivant :
- la clé publique de chiffrement est définie par un module RSA $n = pq$, ainsi qu'un exposant e, premier avec $\varphi(n)$;
- la clé de déchiffrement consiste en l'exposant $d = e^{-1} \bmod \varphi(n)$.
- le chiffrement d'un message $m \in \mathbb{Z}_n^\star$ est $c = m^e \bmod n$;
- le déchiffrement d'un chiffré $c \in \mathbb{Z}_n^\star$ est $m = c^d \bmod n$.

Q-1. Décrire une attaque contre la sécurité sémantique de ce schéma, en précisant sa complexité algorithmique et son avantage.

Rappel : L'avantage $\mathsf{Adv}_\pi^{\mathsf{ind}}(\mathcal{A})$ d'un attaquant $\mathcal{A} = (A_1, A_2)$ contre la sécurité sémantique d'un schéma de chiffrement $\pi = (\mathcal{G}, \mathcal{E}, \mathcal{D})$ est

$$\mathsf{Adv}_\pi^{\mathsf{ind}}(\mathcal{A}) = 2 \times \Pr_{b \xleftarrow{R} \{0,1\}} \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{G}(1^k); (m_0, m_1, s) \leftarrow A_1(\mathsf{pk}) \\ c = \mathcal{E}_{\mathsf{pk}}(m_b) : A_2(m_0, m_1, s, c) = b \end{array} \right] - 1.$$

6.2 Chiffrement D-RSA

On a alors proposé la variante suivante :
- la clé publique de chiffrement est définie par un module RSA $n = pq$, ainsi qu'un exposant e, premier avec $\varphi(n)$;
- la clé de déchiffrement consiste en l'exposant $d = e^{-1} \bmod \varphi(n)$.
- pour le chiffrement d'un message $m \in \mathbb{Z}_n$, on choisit un élément aléatoire r dans $\mathbb{Z}_n$, puis on calcule $a = r^e \bmod n$ ainsi que $b = (r+1)^e \times m \bmod n$. Le couple (a, b) constitue le chiffré.

Q-2. Décrire l'algorithme de déchiffrement, à partir du chiffré (a, b), du module public n et de la clé de déchiffrement d.

6.3 Sécurité prouvée

On définit le problème du *(Computational) Dependent-RSA* – C-DRSA :
étant donné (n, e) et $a = r^e \bmod n$, calculer $(r+1)^e \bmod n$.

Q-3. Montrer que, sous réserve que le problème C-DRSA soit difficile à résoudre, le schéma de chiffrement décrit ci-dessus est non-inversible (soit $\mathsf{OW} - \mathsf{CPA}$).

On définit le problème du *Decisional Dependent-RSA* – D-DRSA :
étant donné (n, e), $a = r^e \bmod n$ et $b = s^e \bmod n$, décider si $s = r + 1 \bmod n$.

Rappel : Un attaquant $\mathcal{A}$ est capable de décider (résoudre le problème D-DRSA) si $\mathsf{Adv}_{n,e}^{\mathsf{ddrsa}}(\mathcal{A})$ est non-négligeable, où

$$\begin{aligned} \mathsf{Adv}_{n,e}^{\mathsf{ddrsa}}(\mathcal{A}) \;=\; & \Pr_{r \in \mathbb{Z}_n} [\mathcal{A}(n, e, r^e \bmod n, (r+1)^e \bmod n) \to 1] \\ & - \Pr_{r,s \in \mathbb{Z}_n} [\mathcal{A}(n, e, r^e \bmod n, s^e \bmod n) \to 1]. \end{aligned}$$

Q-4. Montrer que, sous réserve que ce problème D-DRSA soit difficile à résoudre, le schéma de chiffrement décrit ci-dessus est sémantiquement sûr (soit $\mathsf{IND} - \mathsf{CPA}$).

Q-5. Préciser l'avantage maximum d'un attaquant contre la sécurité sémantique de ce schéma, à clé (n, e) fixée, par rapport à l'avantage maximal contre le problème D-DRSA (soit $\mathsf{Adv}_{n,e}^{\mathsf{ddrsa}}(t)$, l'avantage maximal qu'un attaquant peut obtenir en temps t).

6.4 Non-malléabilité

Malheureusement, on ne peut espérer prouver mieux en terme de sécurité :

Q-6. Décrire un attaquant contre la non-malléabilité de ce schéma (sans entrer dans les détails de la définition de la non-malléabilité, montrer comment de simples relations entre des clairs se transposent en des relations simples entre les chiffrés).

Q-7. Que dire de son niveau de sécurité IND-CCA2 ?

6.5 Amélioration

Pour renforcer le niveau de sécurité, on a alors ajouté un troisième champ $c = H(m, r)$ dans le chiffré : pour le chiffrement d'un message $m \in \mathbb{Z}_n$, on choisit un élément aléatoire r dans $\mathbb{Z}_n$, puis on calcule $a = r^e \bmod n$ ainsi que $b = (r+1)^e \times m \bmod n$, et $c = H(m, r)$. Le triplet (a, b, c) constitue le chiffré.

Q-8. Montrer que si on modélise H par un oracle aléatoire, il est aisé de simuler l'oracle de déchiffrement à partir des questions-réponses de cette fonction H.

Q-9. Que dire de son niveau de sécurité IND-CCA2 ?