4. Chiffrement asymétrique IND-CCA2

4.1 Conversion générique

En 1999, Fujisaki et Okamoto ont proposé une construction générique, conduisant à du chiffrement asymétrique IND-CCA2, à partir d'un chiffrement faible.

Soit un schéma probabiliste $\mathcal{S} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$:

- $\mathcal{K}(1^k)$: retourne un couple de clés $(\mathsf{sk}, \mathsf{pk}) \in \mathcal{SK} \times \mathcal{PK}$.
- $\mathcal{E}_{\mathsf{pk}}(m; r)$: pour un message $m \in \mathcal{M}$ et l'aléa $r \in \mathcal{R}$, retourne le chiffré $c \in \mathcal{C}$ résultant.
- $\mathcal{D}_{\mathsf{sk}}(c)$: pour un chiffré $c \in \mathcal{C}$, retourne le message clair $m \in \mathcal{M}$, ou $\perp$ si le chiffré n'est pas valide.

On dérive le schéma $\mathcal{S}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ suivant, avec deux fonctions de hachage

$$G : \{0,1\}^\star \to \{0,1\}^{k_1} \qquad H : \{0,1\}^\star \to \mathcal{R}$$

- $\mathcal{K}'(1^k)$: exécute $(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathcal{K}(1^k)$, retourne les clés $(\mathsf{sk}, \mathsf{pk})$.
- $\mathcal{E}'_{\mathsf{pk}}(m; r)$: pour un message m de k_1 bits, et un aléa $r \in \mathcal{M}$, on calcule $s = H(m, r)$, puis $c_1 \leftarrow \mathcal{E}_{\mathsf{pk}}(r; s)$. Ensuite, on calcule $c_2 = m \oplus G(r)$. Le chiffré consiste en le couple $C = (c_1, c_2)$.

Q-1. Décrire l'algorithme de déchiffrement $\mathcal{D}'_{\mathsf{sk}}$. Préciser les espaces de départ et d'arrivée.

4.2 Sécurité

On définit, pour tout algorithme $\mathcal{A}$, son succès contre la non-inversibilité :

$$\mathsf{Succ}^{\mathsf{ow-cpa}}_{\mathcal{S}}(\mathcal{A}) = \Pr_{\substack{m \in \mathcal{M} \\ r \in \mathcal{R}}} [(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathcal{K}(1^k) : \mathcal{A}(\mathcal{E}_{\mathsf{pk}}(m; r)) \stackrel{?}{=} m].$$

De même, pour tout algorithme $\mathcal{A}^{\mathcal{D}} = (A_1^{\mathcal{D}}, A_2^{\mathcal{D}})$, qui a accès à l'oracle de déchiffrement $\mathcal{D}$, on définit son avantage contre la sécurité sémantique :

$$\mathsf{Adv}^{\mathsf{ind-cca2}}_{\mathcal{S}}(\mathcal{A}) = \left| 2 \times \Pr_{\substack{b \in \{0,1\} \\ r \in \mathcal{R}}} \left[\begin{array}{l} (\mathsf{sk}, \mathsf{pk}) \leftarrow \mathcal{K}(1^k), (m_0, m_1, \sigma) \leftarrow A_1^{\mathcal{D}}(\mathsf{pk}) \\ c \leftarrow \mathcal{E}_{\mathsf{pk}}(m_b; r) : A_2^{\mathcal{D}}(c, \sigma) \stackrel{?}{=} b \end{array} \right] - 1 \right|.$$

Enfin, $\mathsf{Succ}^{\mathsf{ow-cpa}}_{\mathcal{S}}(t)$ (resp. $\mathsf{Adv}^{\mathsf{ind-cca2}}_{\mathcal{S}}(t)$) désigne le succès (resp. l'avantage) maximal qu'un attaquant peut obtenir en temps t.

Q-2. Montrer le lien qui existe entre $\mathsf{Succ}^{\mathsf{ow-cpa}}_{\mathcal{S}}(t)$ et $\mathsf{Adv}^{\mathsf{ind-cca2}}_{\mathcal{S}'}(t')$, dans le modèle de l'oracle aléatoire (les fonctions G et H sont considérées parfaitement aléatoires).

Pour cela, on fera évoluer la distribution de probabilités qui définit les réponses des oracles aléatoires G et H, ainsi que r et b impliqués pour la sécurité sémantique ($\mathsf{Adv}^{\mathsf{ind-cca2}}$). Puis on étudiera, en fonction des différentes distributions de probabilités, les événements S (la réponse b' de l'attaquant est égale au bit b ci-dessus), AskG (la question $G(r)$ est posée, où r est l'aléa utilisé dans le challenge c), AskH (la question $H(m_b, r)$ est posée) et AskR (r est posé à G ou H, soit $\mathsf{AskR} = \mathsf{AskG} \vee \mathsf{AskH}$).

Dans un premier temps, on rend la vue de l'attaquant indépendante de b, ainsi la probabilité de l'événement S est exactement $1/2$. Ensuite, on simule l'oracle de déchiffrement : On peut, dès le début, transmettre toute question $H(m, r)$ à $G(r)$, et stocker dans les listes Λ_H et Λ_G toutes les questions-réponses obtenues par l'attaquant auprès de H et G. Puis,

1. r^+ et g^+ sont choisis, pour définir respectivement r et $G(r)$, dans le challenge $C = (c_1, c_2)$ (avec $c_2 \leftarrow m_b \oplus g^+$), et pour les réponses de G (avec $G(r) \leftarrow g^+$) ;
2. On conserve $c_2 = m_b \oplus g^+$, mais $G(r)$ est défini indépendamment de g^+ ;
3. s^+ est choisi, pour définir s et donc $H(m_b, r)$, dans le challenge $C = (c_1, c_2)$ (avec $c_1 \leftarrow \mathcal{E}_{\mathsf{pk}}(r, s^+)$), et pour les réponses de H (avec $H(m_b, r) \leftarrow s^+$) ;
4. On conserve $c_1 = \mathcal{E}_{\mathsf{pk}}(r, s^+)$, mais $H(m_b, r)$ est défini indépendamment de s^+ ;
   Quelle est la probabilité de S_4 ?
5. On simule l'oracle de déchiffrement, grâce à la liste Λ_H ;
6. c_1^+ est choisi aléatoirement, pour définir c_1 dans le challenge C. Cela définit alors implicitement r^+ et s^+. On remarquera que AskR_6 est relié à $\mathsf{Succ}^{\mathsf{ow-cpa}}$.

Remarques :

— On pourra utiliser la valeur $\lambda(\mathcal{S})$, définie comme étant le maximum, pour $\mathsf{pk} \in \mathcal{PK}$, $m \in \mathcal{M}$ et $c \in \mathcal{C}$, de $\Pr_{r \in \mathcal{R}}[\mathcal{E}_{\mathsf{pk}}(m; r) = c]$.

— On notera q_G et q_H le nombre de questions posées aux oracles G et H respectivement, ainsi que q_D le nombre de questions posées à l'oracle de déchiffrement $\mathcal{D}'$.

4.3 Chiffrement RSA

On a vu que la primitive RSA, $f_{e,N}(x) = x^e \bmod N$, fournit un schéma de chiffrement OW-CPA. On envisage d'utiliser une version probabiliste de la forme

$$\mathcal{E}_{e,N}(m; r) = f_{e,N}(m) \| r.$$

Q-3. Détailler le schéma de chiffrement $\mathcal{S}$ ainsi obtenu, en précisant les tailles de chaque élément, ainsi que les espaces de départ et d'arrivée.

Q-4. Calculer le niveau de sécurité garanti par ce schéma, soit $\mathsf{Succ}_{\mathcal{S}}^{\mathsf{ow-cpa}}(t)$ en fonction de $\mathsf{Succ}^{\mathsf{rsa}(k)}(t)$, la probabilité d'inverser la fonction RSA sur des modules RSA de k bits en temps t. Puis donner un majorant de $\lambda(\mathcal{S})$. On expliquera alors l'intérêt de « r ».

Q-5. Préciser le schéma $\mathcal{S}'$ qui résulte de l'application de la conversion précédente (présentée section 4.1) à ce schéma $\mathcal{S}$.

Q-6. Évaluer le niveau de sécurité garanti par $\mathcal{S}'$: une borne supérieure de $\mathsf{Adv}_{\mathcal{S}'}^{\mathsf{ind-cca2}}(t)$ en fonction de $\mathsf{Succ}^{\mathsf{rsa}(k)}(t)$.