3. Schémas de chiffrement

3.1 Sécurité sémantique et indistingabilité des chiffrés

En 1984, Goldwasser et Micali ont défini la notion de sécurité sémantique par " tout ce qui peut être calculé efficacement sur le clair avec le chiffré, peut être calculé sans le chiffré. " Ceci peut alors être formalisé de la façon suivante : on considère un attaquant $\mathcal{A} = (A_1, A_2)$ en deux étapes. Dans un premier temps, l'algorithme A_1, à la vue de la clé publique pk, retourne une distribution sur l'ensemble des messages, caractérisée par un algorithme d'échantillonnage M. Un tel algorithme ne doit retourner avec une probabilité non nulle que des messages de même taille. Dans un deuxième temps, l'algorithme A_2 reçoit le chiffré y d'un message aléatoire x (selon la distribution M). Cet adversaire retourne une fonction f, et une valeur α.

Un tel attaquant réussit dans son attaque si $f(x) = \alpha$ avec une meilleure probabilité que sur un message aléatoire inconnu $f(x^\star) = \alpha$.

$$\mathsf{Adv}^{\mathsf{sem}}(\mathcal{A}) = \left|\mathsf{Succ}^{M}(\mathcal{A}) - \mathsf{Succ}^{\$}(\mathcal{A})\right|, \text{ avec}$$

$$\left.\begin{array}{rcl} \mathsf{Succ}^{M}(\mathcal{A}) & = & \Pr\left[\alpha = f(x)\right] \\ \mathsf{Succ}^{\$}(\mathcal{A}) & = & \Pr\left[\alpha = f(x^\star)\right] \end{array}\right\} \begin{array}{l} \text{sur l'espace de probabilités défini par} \\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathcal{K}(1^k), (M, s) \leftarrow A_1(\mathsf{pk}), \\ x, x^\star \leftarrow M, y = \mathcal{E}_{\mathsf{pk}}(x; r), (f, \alpha) \leftarrow A_2(y, M, s). \end{array}$$

Q-1.

- Montrer que la sécurité sémantique est équivalente à l'indistingabilité des chiffrés.
- Montrer que cette équivalence subsiste même si f est restreinte à retourner une sortie binaire.

3.2 Chiffrement de Goldwasser et Micali

En 1984, suite à la définition de la sécurité sémantique, Goldwasser et Micali ont proposé le premier schéma de chiffrement sémantiquement sûr.

- Génération des clés : étant donné un paramètre de sécurité k, on choisit un module RSA N sur k bits, ainsi qu'un non-résidu quadratique $\alpha \in \mathbb{Z}_N^\star$ (comme cas particulier, on peut considérer $N = pq$, où $p, q = 3 \bmod 4$ et $\alpha = -1$.
- Chiffrement d'un bit b : $c = x^2\alpha^b \bmod N$, pour $x \xleftarrow{R} \mathbb{Z}_N^\star$.

Q-2.

- Décrire l'algorithme de déchiffrement.
- Montrer que ce schéma est bien sémantiquement sûr. Préciser l'hypothèse algorithmique nécessaire et suffisante.

3.3 Chiffrement de Paillier

En 1999, Pascal Paillier a proposé une extension du schéma de Goldwasser et Micali, mais dans un contexte particulier : $N = pq$ est la clé publique, puis $\mathcal{E}(m; r) = (1 + N)^m r^N \bmod N^2$.

Q-3.

— Montrer que la fonction

$$\begin{array}{rcccl} f & : & \mathbb{Z}_N \times \mathbb{Z}_N^\star & \to & \mathbb{Z}_{N^2}^\star \\ & & (m, r) & \mapsto & (1+N)^m r^N \bmod N^2 \end{array}$$

est un isomorphisme de groupes.

— Montrer que la factorisation de N permet de l'inverser.

— Montrer que le calcul de racines N-ièmes modulo N permet de l'inverser.

— En déduire l'algorithme de déchiffrement.

— Préciser les hypothèses algorithmiques sur lesquelles reposent les notions OW-CPA et IND-CPA.

3.4 Chiffrement de Rabin

En 1978, Rabin propose une alternative à RSA, basée sur le problème de la racine carrée modulaire.

— Génération des clés : étant donné un paramètre de sécurité k, on choisit un module RSA $N = pq$ sur $2k + 1$ bits.

— Chiffrement d'un message $x \in \mathbb{Z}_N$: $c = x^2 \bmod N$.

Q-4. Décrire l'algorithme de déchiffrement. Montrer qu'une redondance dans le message clair est nécessaire.

On propose la redondance : $x = m \| 0^{k_1}$, où m est le message à chiffrer sur $2k - k_1$ bits, et les k_1 bits de poids faible de x sont imposés à 0.

Q-5. Décrire l'algorithme de déchiffrement associé. La OW-CPA est-elle équivalente à la factorisation ? Exprimer le coût de la réduction en fonction de k_1.