

Notion de Sécurité CCA

Soit $\text{KeyGen}, \text{Enc}, \text{Dec}$ un schéma de chiffrement à clé publique CCA-sûr défini sur $\mathcal{M}, \mathcal{C}$ où $\mathcal{C} = \{0, 1\}^\ell$. Soit $(\text{KeyGen}, \text{Enc}', \text{Dec}')$ un schéma défini sur $\mathcal{M}, \mathcal{C}'$ où $\mathcal{C}' = \{0, 1\}^{\ell+1}$ de la manière suivante :

$$\text{Enc}'(\text{pk}, m) := \text{Enc}(\text{pk}, m) \| 0$$

et

$$\text{Dec}'(\text{sk}, c) := \text{Dec}(\text{sk}, c[0 \dots \ell - 1])$$

autrement dit le dernier bit de chiffré peut être 0 ou 1, mais le déchiffrement l'ignore.

Question 1. *Le chiffrement est-il IND-CPA ?*

Question 2. *Montrer que $(\text{KeyGen}, \text{Enc}', \text{Dec}')$ n'est pas IND-CCA.*

Autour de ElGamal

Rappelons le principe du chiffrement ElGamal.

Soit $\mathbf{G}$ un groupe d'ordre q premier et g un générateur.

KeyGen. Tirer $\text{sk} \leftarrow U([1, q - 1])$ et calculer $\text{pk} = g^{\text{sk}}$.

Enc(m, pk). Tirer $r \leftarrow U(\mathbb{Z}_q)$ et renvoyer $(g^r, m \cdot \text{pk}^r)$.

Dec((c_1, c_2), sk). Renvoyer $c_2 \cdot (c_1)^{-\text{sk}}$.

Question 3. *Montrer que ElGamal est homomorphe pour la multiplication : si $(c_1, c_2) = \text{Enc}(m, \text{pk})$ et $(c'_1, c'_2) = \text{Enc}(m', \text{pk})$ alors $(c_1 c'_1, c_2 c'_2) = \text{Enc}(mm', \text{pk})$.*

Question 4. *ElGamal est-il IND-CCA ?*

Question 5. *La valeur aléatoire r (« sel ») peut-elle être réutilisée pour un autre message ?*

Question 6. *Soit p, q de grands premiers tels que q divise $p - 1$. Soit $\mathbf{G}$ le sous-groupe de $\mathbb{Z}_p^*$ d'ordre q engendré par g et supposons que DDH est difficile dans $\mathbf{G}$.*

Supposons que nousinstancions le système ElGamal dans le groupe $\mathbf{G}$; cependant les messages sont pris dans le groupe $\mathbb{Z}_p^$ entier. Montrer que le système qui résulte de ce choix n'est pas IND-CPA.*

Pendant des décennies, la question de savoir si ElGamal était IND-CCA1 est restée ouverte. On sait aujourd'hui qu'on ne peut pas prouver sa sécurité IND-CCA1 sous des hypothèses standard ("New limits of provable security and applications to ElGamal encryption", Schäge, EUROCRYPT 2024).

Une variante de RSA (*)

Le problème RSA est le suivant.

Problem 1. *Soit $N = pq$ où p, q sont premiers, e premier avec $\phi(N)$ et y , trouver x tel que $x^e = y \pmod{N}$.*

Considérons le schéma ci-dessous, où H est une fonction de hachage « idéale ».

KeyGen. Le même que textbook RSA : $\text{pk} := (e, N)$ et $\text{sk} := (d, N)$ où $ed = 1 \pmod{\phi(N)}$.

Enc(m, pk). Tirer $r \leftarrow U(\mathbb{Z}_N)$ et renvoyer $(r^e, H(r)m) \in \mathbb{Z}_N^2$.

Dec($(c_1, c_2), \text{sk}$). Renvoyer $c_2(H(c_1^d))^{-1} \in \mathbb{Z}_N$.

Question 7. Montrer que le schéma est correct.

Question 8. Montrer qu'on peut utiliser un adversaire contre le problème RSA pour monter un adversaire contre le jeu IND-CPA.

La fonction H est considérée se comporter comme un *oracle aléatoire*. Ainsi, dans les preuves de sécurité suivantes, on supposera que chaque fois qu'un calcul de H est effectué sur une entrée x :

- si x a déjà été vu, on renvoie la même valeur $H(x)$ que précédemment ;
- sinon, $H(x)$ est sélectionné uniformément au hasard.

Question 9. Soit G le jeu IND-CPA joué entre le challenger $\mathcal{C}$ et l'attaquant $\mathcal{A}$. Soit G' une modification de ce jeu dans lequel le chiffré challenge $c_1, c_2 = (r^e, H(r)m_b)$ est modifié comme suit : $H(r)$ est remplacé par une valeur aléatoire indépendante de r .

Soit E l'évènement dans le jeu G' :

« $\mathcal{A}$ appelle H sur l'entrée r »

Justifier que tant que l'évènement E ne se produit pas, la vue de l'adversaire dans le jeu G et dans le jeu G' sont identiques.

Question 10. Justifier que :

$$\Pr[\mathcal{A} \text{ gagne } G'] = \frac{1}{2}$$

Question 11. Dédurre des questions précédentes que :

$$\left| \Pr[\mathcal{A} \text{ gagne } G] - \frac{1}{2} \right| \leq \Pr[E] \quad .$$

Question 12. Soit $\mathcal{A}$ un adversaire IND-CPA contre le schéma proposé. On construit un adversaire $\mathcal{B}$ contre le problème RSA comme suit.

$\mathcal{B}$ exécute localement $\mathcal{A}$. Pendant cette exécution, $\mathcal{A}$ «croit» se trouver dans le jeu G' .

- Chaque fois que $\mathcal{A}$ fait un appel à H , on enregistre la valeur d'appel.
- $\mathcal{A}$ choisit une paire de messages m_0, m_1
- Lorsque $\mathcal{B}$ reçoit la valeur y , il envoie $(y, *m_b)$ à $\mathcal{A}$, où $*$ est une nouvelle valeur aléatoire.
- Enfin, quand $\mathcal{A}$ termine, $\mathcal{B}$ renvoie une des valeurs d'appel prise au hasard.

On suppose qu'au maximum t requêtes à H sont faites. Soit E l'évènement défini plus haut, qui concerne donc $\mathcal{A}$. Montrer que :

$$\Pr[\mathcal{B} \text{ gagne}] \geq \frac{1}{t} \Pr[E] \quad .$$

Question 13. Montrer que le schéma proposé est IND-CPA sous l'hypothèse que le problème RSA est difficile.