Séance 4 - Travaux Dirigés
Réductions et Définitions de sécurité

Yann Rotella

2026

Échauffement seul.e - une heure

Exercice 1. *Définitions de sécurité - IND-CPA.*
Dans cet exercice, nous allons reposer les bases des définitions de sécurité vues en cours

(1) Rappeler ce qu'est un chiffrement IND-CPA.

(2) Dans la pratique, et pour des raisons d'efficacité, les chiffrements préservent la longueur. Montrer alors que, pour des messages de longueurs différentes, le chiffrement ne peut être IND-CPA.

Dans la suite, on ne va considérer que des messages de même taille. Et on ne considère aucune propriété sur le chiffrement.

(3) Pour un adversaire $\mathcal{A}$, donner son avantage dans ce contexte si l'attaquant peut réaliser N calculs du chiffrement E.

(4) Même question si l'adversaire peut réaliser M pré-calculs et ne réalise aucun autre calcul.

Exercice 2. *Réel ou aléatoire en chiffrés choisis.*
L'idée de l'exercice ici est de formaliser un jeu de sécurité qui « capturerait » la possibilité d'un attaquant d'observer aussi des clairs correspondant à des chiffrés de son choix.

(1) Rappeler ce qu'est un chiffrement indistinguable de l'aléatoire à clairs choisis.

(2) Modifier cette définition afin de modéliser un attaquant qui pourrait observer des clairs correspondant à des chiffrés de son choix.

(3) On peut imaginer encore plus fort : IND-CCA adaptatif : donner une définition de jeu de sécurité où l'attaquant est capable de choisir des messages ou des chiffrés de manière adaptative par rapport à ce qu'il observe.

En groupes de 3 - à vous de jouer

Exercice 3. *PRG sûrs ou non ?.*
Un PRG (Pseudo Random Generator), générateur pseudo-aléatoire est une fonction G de $\{0,1\}^s$ dans $\{0,1\}^n$ avec $n > s$ dont la sortie doit être indistinguable d'une suite aléatoire. Soit G un PRG sécurisé.

(1) Donner le jeu de sécurité associé.

(2) Donner l'avantage de l'attaquant si celui-ci peut réaliser N calculs de G.

(3) Montrer que pour toute permutation P dont on connaît un calcul de l'inverse P^{-1}, $P \circ G$ est un PRG sécurisé. Que pouvez-vous conclure de cela en pratique ?

(4) Montrer que n'importe quelle sélection des bits de sortie de G donne un PRG sécurisé.

(5) Montrer que $G' : \{0,1\}^s \to \{0,1\}^{n+s}$ tel que pour tout $x \in \{0,1\}^s$, $G'(x) = G(x)||x$ n'est pas un PRG sécurisé. Que pouvez-vous en conclure en pratique ?

Exercice 4. *PRF et recherche exhaustive.*
On considère une famille de fonctions $\mathcal{F}$ dont les entrées sont de n bits et les sorties de m bits, paramétrée par une clef $k \in \{0,1\}^\kappa$.

(1) Décrire $\mathcal{F}$ mathématiquement.

(2) Pour un adversaire $\mathcal{A}$, décrire le jeu de sécurité de distinguabilité de $\mathcal{F}$ et donner son avantage.

(3) Décrire un adversaire qui peut réaliser 2^κ calculs (de fonctions dans $\mathcal{F}$) et dont l'avantage est proche de 1.

(4) Approcher l'avantage de l'adversaire si celui-ci est limité à 2^j calculs.

Exercices complémentaires

Exercice 5. *Mode compteur et IND-CPA.*
On va essayer de capturer tout ce qu'il ne faudrait pas faire dans le cas du mode compteur. On suppose que le mode compteur est instancié avec une PRF dont l'entrée est sur n bits. Les messages font toujours la même taille.

(1) Rappeler la construction du mode compteur.

(2) Rappeler pourquoi l'IV doit être pris aléatoirement.

(3) Montrer que si l'IV du mode compteur est limité à deux octets, alors le chiffrement associé n'est pas IND-CPA. Donner la stratégie d'attaque, l'avantage et la complexité.

(4) Montrer que, si le compteur est limité à un octet, alors le chiffrement associé n'est pas IND-CPA. Donner la stratégie d'attaque, l'avantage et la complexité.

(5) Montrer que si $n = 32$, le mode compteur n'est pas IND-CPA. Donner une stratégie d'attaque, l'avantage et la complexité.

Exercice 6. *PRFs.*
Soit $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ une PRF sécurisée et soit $F' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ telle que

$$F'(k,x) = F(k,x) \oplus F(k, x \oplus 1^n)$$

(1) Montrer que F' n'est pas une PRF sécurisée

On propose maintenant de construire la fonction $F'' : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ telle que

$$F''(k_1,k_2,x) = F(k_1,x) \oplus F(k_2,x)$$

(2) Montrer que F'' est une PRF sécurisée.

On choisit maintenant $F^{(3)}$ qui consiste simplement à tronquer la sortie de F.

(3) Montrer que $F^{(3)}$ est une PRF sécurisée.