

DÉFINITIONS DE SÉCURITÉ

ORACLES, RÉDUCTIONS, DÉFINITIONS

Yann Rotella

UVSQ - Université Paris-Saclay

12 février 2026



PLAN DU COURS

DÉFINITIONS DE SÉCURITÉ

PRIMITIVES

LE MODE COMPTEUR

DÉFINITIONS DE SÉCURITÉ

IND-CPA

Réel ou aléatoire

PRIMITIVES

Pseudo-Random Functions (PRFs)

Pseudo-Random Generators

Pseudo-Random Permutations

LE MODE COMPTEUR

Définition

Sécurité

Preuve

CPA - CHOSEN PLAINTEXT ATTACKS - NOTION DE SÉCURITÉ

On considère un schéma de chiffrement symétrique

$$\text{Enc} : \{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^*$$

On cherche à **capturer** la **résistance** à des attaques à clairs choisis.

✍ À quels autres modèles d'attaque cela garantira la sécurité ?

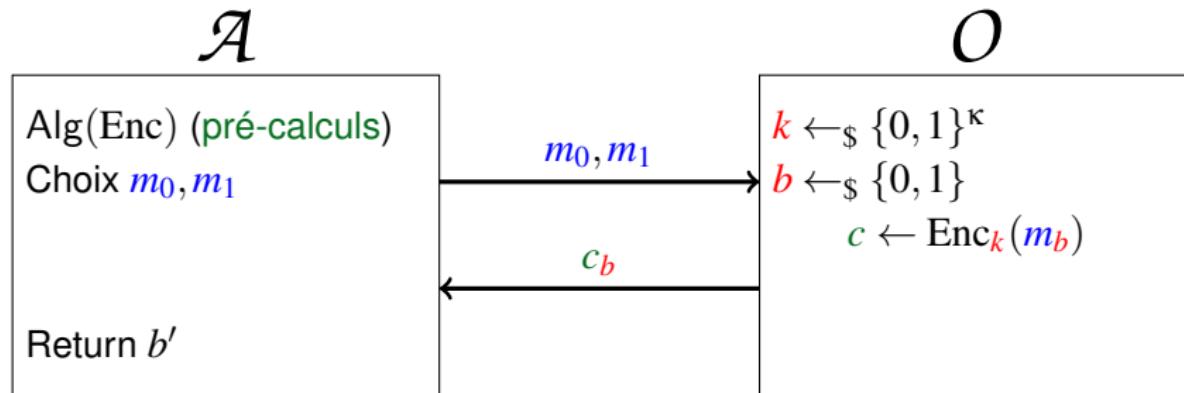
L'attaquant peut donc choisir des messages m_1, m_2, \dots, m_n et observer leur chiffré correspondant.

✍ À partir de là qu'est-ce qu'on ne veut pas que l'attaquant soit capable de faire ?

IND-CPA - DÉFINITION

L'adversaire \mathcal{A} connaît Enc. La clef secrète k est tirée aléatoirement dans $\{0, 1\}^k$.

L'adversaire est limité en **calculs**.



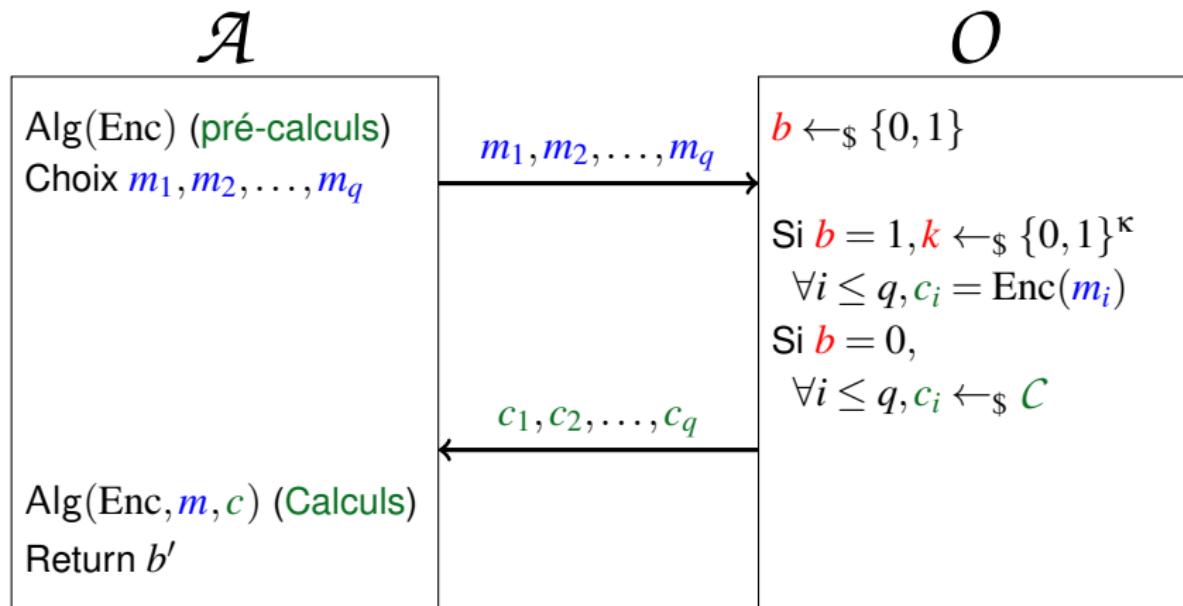
L'**avantage** de l'attaquant est défini par

$$\text{Adv}(\mathcal{A}) = |2\Pr[b' = b] - 1|$$

DÉFINITIONS DE SÉCURITÉ

- ▶ Plusieurs (IND-CCA1, IND-CCA2)
- ▶ Permet de réaliser des **réductions** de sécurité
- ▶ PRP, PRF, PRG

UNE AUTRE DÉFINITION - RÉEL OU ALÉATOIRE



RÉEL OU ALÉATOIRE EST SUFFISANT

THÉORÈME (RÉDUCTION RÉEL OU ALÉATOIRE ET IND-CPA)

Si un schéma de chiffrement résiste au jeu Réel ou Aléatoire, alors il est IND-CPA.

 Preuve informelle au tableau

DÉFINITIONS DE SÉCURITÉ

IND-CPA

Réel ou aléatoire

PRIMITIVES

Pseudo-Random Functions (PRFs)

Pseudo-Random Generators

Pseudo-Random Permutations

LE MODE COMPTEUR

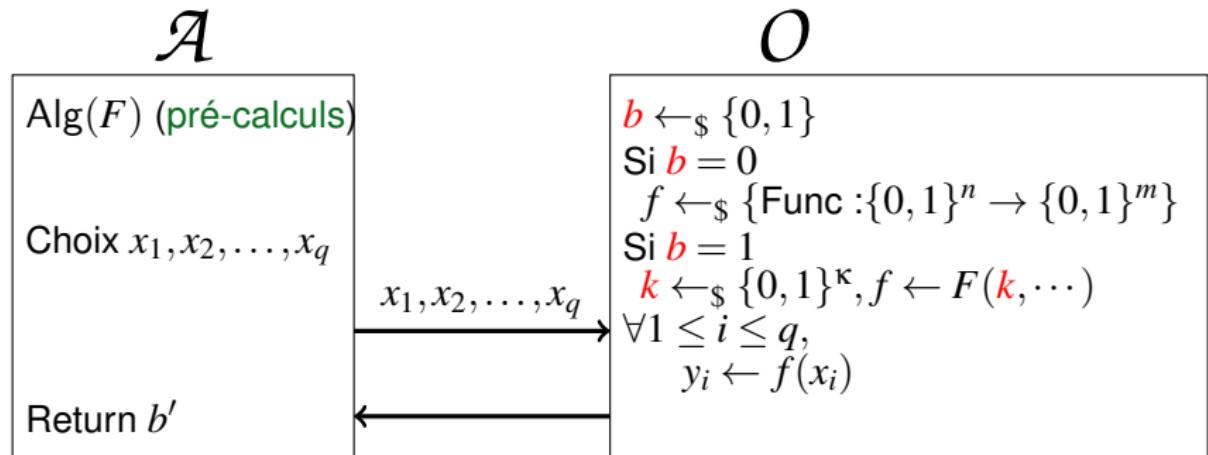
Définition

Sécurité

Preuve

PSEUDO-RANDOM FUNCTIONS

Soit $F : \{0, 1\}^{\kappa} \times \{0, 1\}^n \rightarrow \{0, 1\}^m$ une famille de fonctions paramétrées par une clef.



$$\text{PRFAdv}(\mathcal{A}, \mathcal{F}) = |2\Pr[b' = \mathbf{b}] - 1|$$

PRGs ET PRPs

Un **générateur pseudo-aléatoire** est défini par $G : \{0,1\}^s \rightarrow \{0,1\}^\ell$ où $s < \ell$. Le but de l'attaquant est de **distinguer** la suite sortie du PRG par une valeur (inconnue) de graine ou d'une suite aléatoire.

Une **permutation pseudo-aléatoire** est une famille de permutations, dont la définition est similaire à la notion de fonction pseudo-aléatoire, mais en rajoutant le caractère « **bijectif** ».

- ✍ Faire la définition de sécurité d'un générateur pseudo-aléatoire.
- ✍ Donner des valeurs limites en pratique pour q (le nombre de données).
- ✍ Comment garantir le fait d'avoir une PRF ou une PRP ou une PRG ?

UN CHIFFREMENT PRATIQUE SÉCURISÉ (POUR UN SEUL MESSAGE DE LONGUEUR FIXE)

On considère ici que l'on a accès à un générateur pseudo-aléatoire (PRG), dont l'avantage de tout attaquant est négligeable. On rappelle :

$$G : \{0,1\}^s \rightarrow \{0,1\}^\ell$$

Le schéma de chiffrement symétrique considéré est le suivant :

- ▶ $\textcolor{red}{k} \leftarrow_{\$} \{0,1\}^s$
- ▶ $\textcolor{green}{c} = G(\textcolor{red}{k}) \oplus \textcolor{blue}{m}$

On peut montrer que si G est un PRG, alors ce système est sécurisé pour un seul message.

- ☞ Expliquer pourquoi ce système n'est pas IND-CPA.
- ☞ Idée générale des preuves par réduction.

DÉFINITIONS DE SÉCURITÉ

IND-CPA

Réel ou aléatoire

PRIMITIVES

Pseudo-Random Functions (PRFs)

Pseudo-Random Generators

Pseudo-Random Permutations

LE MODE COMPTEUR

Définition

Sécurité

Preuve

LE MODE COMPTEUR

On suppose l'existence d'une PRF (ou PRP) et on utilise la construction suivante pour chiffrer des messages. On a donc

- ✍ Rappeler la définition d'une PRF.

Pour chiffrer $m \in \{0,1\}^*$, on tire une valeur aléatoire ctr , on calcule $F(k, ctr) || F(k, ctr + 1) || \dots$. On ajoute à cette suite le message m .

- ✍ Dessiner le schéma du mode CTR

SÉCURITÉ DU MODE COMPTEUR

THÉORÈME (RÉDUCTION DU MODE COMPTEUR)

Si F est une PRF, alors le mode compteur est IND-CPA sécurisé

THÉORÈME (RÉDUCTION DU MODE COMPTEUR)

Pour tout adversaire \mathcal{A} contre le mode compteur qui tourne en temps t_A et nécessite q requêtes de longueur ℓ , il existe un adversaire \mathcal{B} tel que

$$\text{Adv}_{CTR}^{IND-CPA}(\mathcal{A}) \leq \text{Adv}_F^{PRF}(\mathcal{B}) + \frac{q^2\ell}{2^n}$$

où \mathcal{B} tourne en temps $t_B = t_A + O(nq\ell)$ et demande au plus $q_B = q\ell$ requêtes à la PRF F

- ☞ Implication si F est une PRF ?
- ☞ Exemple avec $n = 128, \ell = 1kB = 2^6$ et $q = 2^{40}$?

PREUVE (TRÈS) SIMPLIFIÉE

$$\text{Adv}_{CTR}^{IND-CPA}(\mathcal{A}) \leq \text{Adv}_F^{PRF}(\mathcal{B}) + \frac{q^2 \ell}{2^n}$$

$\textcolor{blue}{m}[0]$	$\textcolor{blue}{m}[1]$	\cdots	$\textcolor{blue}{m}[\ell]$
--------------------------	--------------------------	----------	-----------------------------



$F_{\textcolor{red}{k}}[ctr]$	$F_{\textcolor{red}{k}}[ctr + 1]$	\cdots	$F_{\textcolor{red}{k}}[ctr + \ell]$
-------------------------------	-----------------------------------	----------	--------------------------------------



$\textcolor{green}{c}[0]$	$\textcolor{green}{c}[1]$	\cdots	$\textcolor{green}{c}[\ell]$
---------------------------	---------------------------	----------	------------------------------

PREUVE (TRÈS) SIMPLIFIÉE

$$\text{Adv}_{CTR}^{IND-CPA}(\mathcal{A}) \leq \text{Adv}_F^{PRF}(\mathcal{B}) + \frac{q^2 \ell}{2^n}$$

$m[0]$	$m[1]$	\cdots	$m[\ell]$
--------	--------	----------	-----------



$\rho[ctr]$	$\rho[ctr + 1]$	\cdots	$\rho[ctr + \ell]$
-------------	-----------------	----------	--------------------



$c[0]$	$c[1]$	\cdots	$c[\ell]$
--------	--------	----------	-----------

QUELLES SONT LES REQUÊTES ?

► m_1, m_2, \dots, m_q

$ctr_1, ctr_1 + 1, \dots, ctr_1 + \ell - 1$

$ctr_2, ctr_2 + 1, \dots, ctr_2 + \ell - 1$

...

$ctr_q, ctr_q + 1, \dots, ctr_q + \ell - 1$

↳ Expliquer comment choisir ctr .

↳ Que se passe-t'il si toutes les valeurs ci-dessus sont différentes ?
Que se passe t'il si deux valeurs sont égales ?

BORNER LA PROBABILITÉ DE COLLISION

$$\Pr[\exists \text{collision}] = \Pr[\text{Coll}_1 \vee \text{Coll}_2 \vee \text{Coll}_q]$$

$$\Pr[\exists \text{collision}] \leq \Pr[\text{Coll}_1] + \Pr[\text{Coll}_2] + \cdots \Pr[\text{Coll}_q]$$

- ↳ À quelle condition y'a t'il une collision à la première requête ?
- ↳ Comment borner $\Pr[\text{Coll}_2]$?
- ↳ Comment borner $\Pr[\text{Coll}_i]$?
- ↳ En déduire la borne du théorème.

ENLEVER LES COLLISIONS : UTILISATION DU NONCE

DÉFINITION (NONCE)

Number Used Once

- ✍ Dans le cas du mode compteur, en supposant le nombre de blocs inférieur à 2^{64} et une taille d'entrée de 128 bits, donner une manière d'utiliser un nonce afin d'enlever les collisions.

CONCLUSIONS

- ▶ Notions de sécurité bien définies : IND-CPA, IND-CCA1 et 2
- ▶ Preuves par réduction, arguments par contraposée
- ▶ On ne « descend » pas plus que PRF, PRP et PRG
- ▶ On ne sait pas montrer qu'une famille de fonctions est une PRP, PRF, PRG sans hypothèse autre
- ▶ Difficile de quantifier les avantages exacts
- ▶ Arguments asymptotiques sur les constructions
- ▶ On « réduit » la sécurité à quelque chose de « plus facile » à étudier

CONCLUSIONS

- ▶ Modes opératoires, se réduisent à l'analyse de la PRF, PRP utilisée
- ▶ Nécessité de rajouter de l'« aléa » (Nonce, IV) dans le chiffrement !

Au prochain Cours :

- ▶ Diffusion et Confusion
- ▶ Constructions de chiffrements par bloc