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

$$\text{Enc} : \{0,1\}^{\kappa} \times \{0,1\}^{*} \to \{0,1\}^{*}$$

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 $m_1, m_2, \ldots, m_n$ 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 $\{0,1\}^{\kappa}$.

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

$\mathcal{A}$		$\mathcal{O}$
$\mathrm{Alg}(\mathrm{Enc})$ (pré-calculs)		$k \leftarrow_{\$} \{0,1\}^{\kappa}$
Choix m_0, m_1	$\xrightarrow{m_0, m_1}$	$b \leftarrow_{\$} \{0,1\}$
		$c \leftarrow \mathrm{Enc}_k(m_b)$
	$\xleftarrow{c_b}$	
Return b'		

L'avantage de l'attaquant est défini par

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

Définitions de Sécurité

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

Une autre définition - réel ou aléatoire

$\mathcal{A}$

Alg(Enc) (pré-calculs)

Choix $m_1, m_2, \ldots, m_q$

$\xrightarrow{m_1, m_2, \ldots, m_q}$

$\xleftarrow{c_1, c_2, \ldots, c_q}$

Alg(Enc, m, c) (Calculs)

Return b'

$\mathcal{O}$

$b \leftarrow_\$ \{0,1\}$

Si $b = 1, k \leftarrow_\$ \{0,1\}^\kappa$

$\forall i \leq q, c_i = \mathrm{Enc}(m_i)$

Si $b = 0,$

$\forall i \leq q, c_i \leftarrow_\$ C$

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

Pseudo-Random Functions

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

$\mathcal{A}$

Alg(F) (pré-calculs)

Choix $x_1, x_2, \ldots, x_q$

Return b'

$\xrightarrow{x_1, x_2, \ldots, x_q}$

$\longleftarrow$

O

$b \leftarrow_\$ \{0,1\}$
Si $b = 0$
$f \leftarrow_\$ \{$Func :$\{0,1\}^n \to \{0,1\}^m\}$
Si $b = 1$
$k \leftarrow_\$ \{0,1\}^\kappa, f \leftarrow F(k, \cdots)$
$\forall 1 \leq i \leq q,$
$y_i \leftarrow f(x_i)$

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

PRGs et PRPs

Un générateur pseudo-aléatoire est défini par $G : \{0,1\}^s \to \{0,1\}^\ell$ 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 :

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

Le schéma de chiffrement symétrique considéré est le suivant :

- $k \leftarrow_\$ \{0,1\}^s$
- $c = G(k) \oplus m$

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.

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 $F(k, ctr)||F(k, ctr+1)|| \cdots$. 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

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

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

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

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

$$\bigoplus$$

$F_k[ctr]$	$F_k[ctr+1]$	$\cdots$	$F_k[ctr+\ell]$

$$=$$

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

Preuve (très) simplifiée

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

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

$$\bigoplus$$

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

$$=$$

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

Quelles sont les requêtes ?

- $m_1, m_2, \ldots, m_q$

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

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

$$\ldots$$

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

✍ 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

$$\mathsf{Pr}[\exists collision] = \mathsf{Pr}[Coll_1 \vee Coll_2 \vee Coll_q]$$

$$\mathsf{Pr}[\exists collision] \leq \mathsf{Pr}[Coll_1] + \mathsf{Pr}[Coll_2] + \cdots \mathsf{Pr}[Coll_q]$$

- ✍ À quelle condition y'a t'il une collision à la première requête ?
- ✍ Comment borner $\mathsf{Pr}[Coll_2]$?
- ✍ Comment borner $\mathsf{Pr}[Coll_i]$?
- ✍ 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