Cours 3. Primitives symétriques

HAI709I – Cryptographie

Bruno Grenet

Université de Montpellier – Faculté des Sciences

Plan du cours

Résumé du cours précédent

- Formalisation du chiffrement symétrique
- Définition de notions de sécurité
- Constructions théoriques basées sur les générateurs et permutations pseudo-aléatoires

Plan du cours

Résumé du cours précédent

- Formalisation du chiffrement symétrique
- Définition de notions de sécurité
- Constructions théoriques basées sur les générateurs et permutations pseudo-aléatoires

Et en pratique, ça donne quoi ?

Plan du cours

Résumé du cours précédent

- Formalisation du chiffrement symétrique
- Définition de notions de sécurité
- Constructions théoriques basées sur les générateurs et permutations pseudo-aléatoires

Et en pratique, ça donne quoi ?

Ce cours

- Chiffrement par flot :
  - produire des bits pseudo-aléatoires
  - exemple des registres à décalage à rétroaction linéaire (LFSR)
- Chiffrement par bloc :
  - chiffrer un bloc de taille fixée
  - modes opératoires : chiffrer plusieurs blocs
  - exemple de l'AES

1. Chiffrement par flot

2. Chiffrement par bloc

Principes du chiffrement par flot

- Inspiré du chiffrement de Vernam :
  - production d'un masque *à la volée*
  - pendant pratique des constructions basées sur les générateurs pseudo-aléatoires

Principes du chiffrement par flot

- Inspiré du chiffrement de Vernam :
  - production d'un masque *à la volée*
  - pendant pratique des constructions basées sur les générateurs pseudo-aléatoires

Définition

Un chiffrement par flot est un couple d'algorithmes déterministes (Init, Next) tels que

- Init prend en entrée une graîne s et un *vecteur d'initialisation IV* (optionnel), et renvoie un *état initial* st
- Next prend en entrée un état st et renvoie un bit y et un nouvel état st'

Principes du chiffrement par flot

- Inspiré du chiffrement de Vernam :
  - production d'un masque *à la volée*
  - pendant pratique des constructions basées sur les générateurs pseudo-aléatoires

Définition

Un chiffrement par flot est un couple d'algorithmes déterministes (Init, Next) tels que

- Init prend en entrée une graîne s et un *vecteur d'initialisation* IV (optionnel), et renvoie un *état initial* st
- Next prend en entrée un état st et renvoie un bit y et un nouvel état st'

Remarques

- Chiffrement par flot = générateur pseudo-aléatoire *infini*
- IV permet de chiffrer plusieurs messages avec une seule clef
- y peut être plus qu'un bit : $(y, \mathrm{st}') \leftarrow \mathrm{Next}_\ell(\mathrm{st})$ produit ℓ bits

Utilisation en mode synchrone

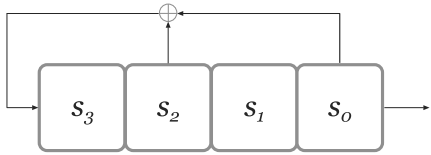
Fonctionnement

- Un émetteur et un récepteur partagent une clef secrète k, et initialisent $\mathrm{st}_0 \leftarrow \mathrm{Init}(k)$
- Quand l'émetteur veut envoyer m de ℓ bits :
  - il calcule $(y, \mathrm{st}'_E) \leftarrow \mathrm{Next}_\ell(\mathrm{st}_E)$ (où st_E est son état courant)
  - il envoie $c = m \oplus y$
- Quand le récepteur reçoit c de ℓ bits :
  - il calcule $(y, \mathrm{st}'_R) \leftarrow \mathrm{Next}_\ell(\mathrm{st}_R)$ (où st_R est son état courant)
  - il déchiffre $m = c \oplus y$

Propriété

- Si aucun message n'est perdu, émetteur et récepteur restent *synchronisés* ($\mathrm{st}_E = \mathrm{st}_R$)
- Fournit un *canal de communication sécurisé* (dans un sens)
- Exemple d'utilisation : GSM, Bluetooth, ...

Registres à décalage à rétroaction linéaire (LFSR)



Définition

- n registres booléens $s_{n-1}, \ldots, s_0$
- n coefficients booléens de rétroaction $c_{n-1}, \ldots, c_0$
- État courant : st $= (s_{n-1}, \ldots, s_0)$
- Init(k) : st $\leftarrow (k_{[n-1]}, \ldots, k_{[0]})$ (pas d'IV)
- Next : $(s_{n-1}, \ldots, s_0) \rightarrow (\bigoplus_i c_i s_i, s_{n-1}, \ldots, s_1)$ et s_0 comme bit de sortie

Remarque

- k est une clef secrète ; les c_i sont connus

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Attaques possibles et linéarité

Force brute

$2^n - 1$ état non nuls $\rightarrow$ cycle de longueur $\leq 2^n - 1$

- longueur du cycle fixée par les coefficients de rétroaction
- restriction aux LFSR de longueur maximale, avec n suffisamment grand

Attaque linéaire

- n premiers bits produits : état initial…
- n bits suivants :

$$y_n = c_{n-1}y_{n-1} \oplus \cdots \oplus c_0 y_0$$

$$\vdots$$

$$y_{2n-1} = c_{n-1}y_{2n-2} \oplus \cdots \oplus c_0 y_{n-1}$$

$\rightarrow$ équation linéaire *modulo* 2 : fournit l'état initial !

Attaques possibles et linéarité

Force brute

$2^n - 1$ état non nuls $\rightarrow$ cycle de longueur $\leq 2^n - 1$

- longueur du cycle fixée par les coefficients de rétroaction
- restriction aux LFSR de longueur maximale, avec n suffisamment grand

Attaque linéaire

- n premiers bits produits : état initial…
- n bits suivants :

$$y_n = c_{n-1}y_{n-1} \oplus \cdots \oplus c_0 y_0$$

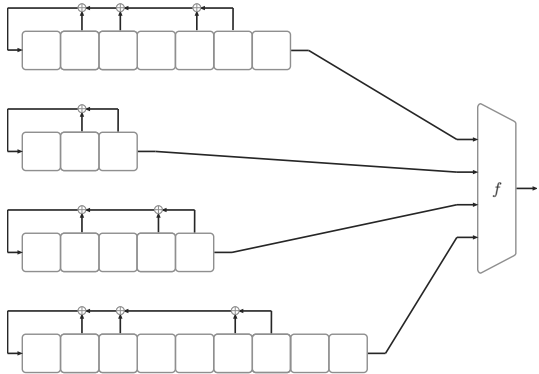
$$\vdots$$

$$y_{2n-1} = c_{n-1}y_{2n-2} \oplus \cdots \oplus c_0 y_{n-1}$$

$\rightarrow$ équation linéaire *modulo* 2 : fournit l'état initial !

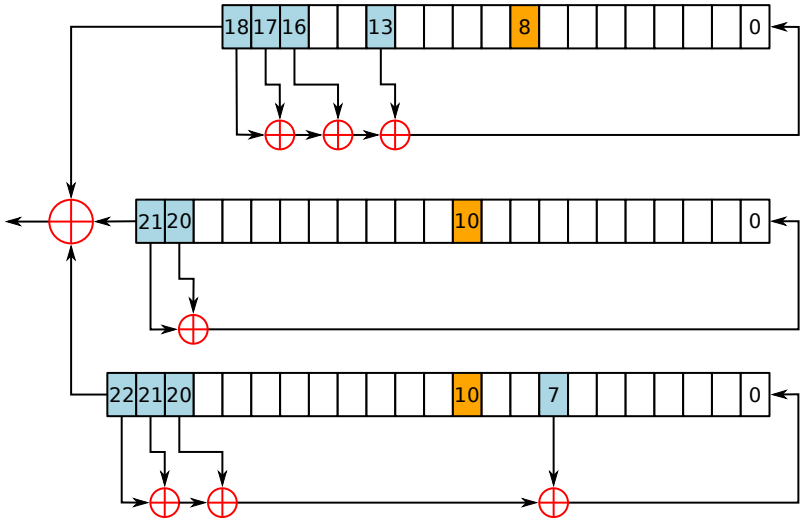
Un LFSR seul n'est pas sûr ! (Et cacher les c_i ne règle rien : algo. de Berlekamp-Massey)

Combiner plusieurs LFSR



- $f : \{0,1\}^t \to \{0,1\}$
- Faciles à mettre en œuvre, rapides
- Très répandu : A5/1 (GSM), E0 (Bluetooth), …
- Difficiles à (bien) concevoir

Exemple A5/1



Source : Wikipédia

1. Chiffrement par flot

2. Chiffrement par bloc

Permutation pseudo-aléatoire

$$F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$$

telle que pour tout k, F_k définie par $F_k(x) = F(k,x)$ est une permutation

On fixe n et ℓ : clefs et blocs de tailles fixées

Permutation pseudo-aléatoire

$$F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$$

telle que pour tout k, F_k définie par $F_k(x) = F(k,x)$ est une permutation

On fixe n et ℓ : clefs et blocs de tailles fixées

Pseudo-aléatoire : difficile à distinguer d'une permutation aléatoire

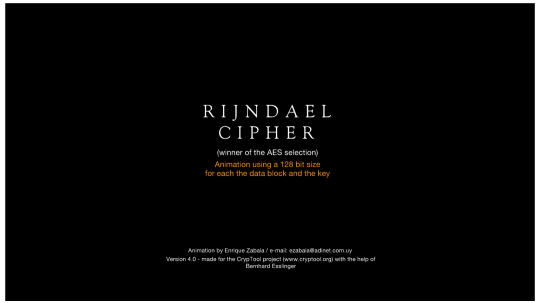
- Définition asymptotique similaire aux générateurs pseudo-aléatoires
- Cas pratique (*sécurité concrète*) : meilleure attaque connue $\to$ force brute, mieux ?

Deux questions

- Comment construire F sûre ?
- Comment utiliser F pour chiffrer des messages de longueur quelconque ?

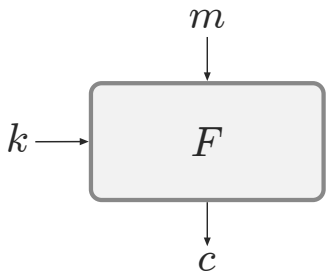
Exemple : AES

- Compétition du NIST 1997-2000
- Vainqueur : Rijndael, de V. Rijmen et J. Daemen
- Chiffrement de blocs de 128 bits, avec clef de taille 128 ou 192 ou 256 (3 versions)
- Basé sur l'idée des réseaux de permutations-substitutions



Source : https://formaestudio.com/portfolio/aes-animation/

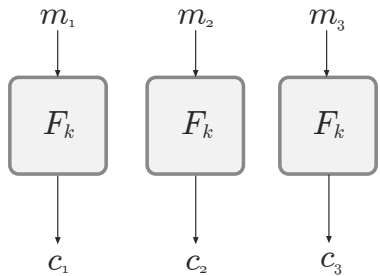
Les modes opératoires



- Un chiffrement par bloc permet de chiffrer des blocs de ℓ bits
- Comment chiffrer plusieurs blocs ?

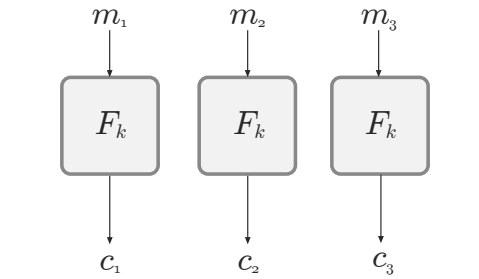
La question n'est en fait pas stupide !

Dictionnaire de codes (ECB)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

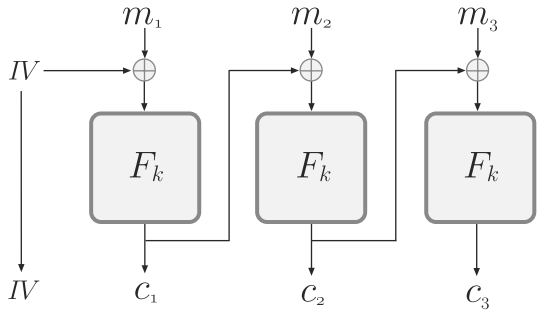
Dictionnaire de codes (ECB)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

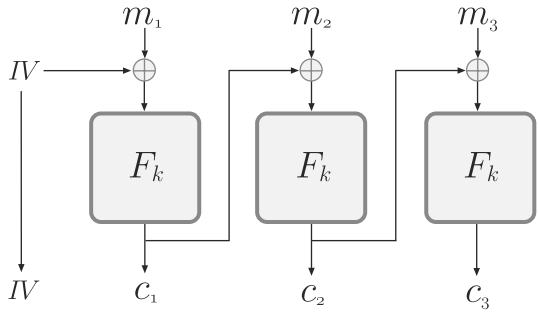
Source : Wikipédia (modif.)

Enchaînement des blocs (CBC)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

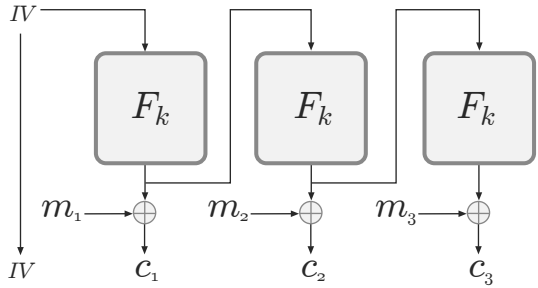
Enchaînement des blocs (CBC)



- Chiffrement CPA-sûr si F est une permutation pseudo-aléatoire
- Inconvénient : chiffrement séquentiel

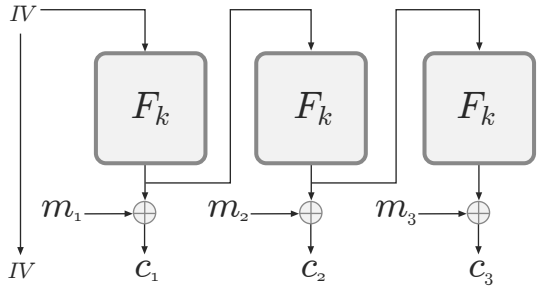
Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Rétroaction de sortie (OFB)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

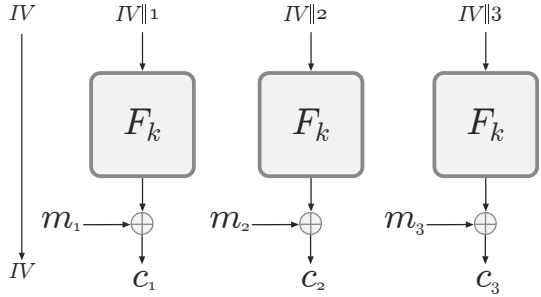
Rétroaction de sortie (OFB)



- Chiffrement CPA-sûr si F est une permutation pseudo-aléatoire
- Toujours séquentiel, mais pré-calculs possibles
- Peut-être vu comme du chiffrement par flot basé sur du chiffrement par blocs

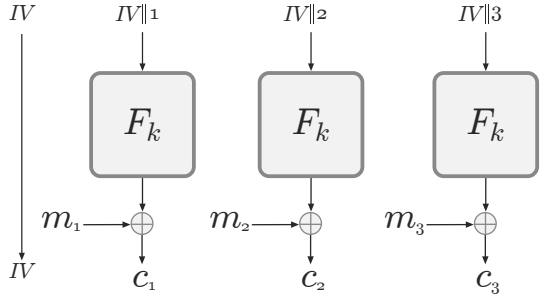
Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Compteur (CTR)



Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Compteur (CTR)



- Purement parallèle !

Théorème

Si F est pseudo-aléatoire, chiffrement CPA-sûr pour les chiffrements multiples

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Preuve pour CTR

CPA-sécurité pour chiffrements multiples :

$Exp(n)$:

1. $k \leftarrow Gen(1^n)$
2. $b \leftarrow$ bit aléatoire
3. A_0 produit des couples (m_0, m_1) et reçoit $c = Enc_k(m_b)$
4. A_0 devine b' et gagne si $b' = b$

CPA-sûr si pour APP A_0, $P_r[A_0 \text{ renvoie } b' = b] \leq \frac{1}{2} + negl(n)$

Preuve pour CTR

Fonction pseudo-aléatoire

- Algo à oracle F : algo D qui peut demander la valeur de $F(x)$ pour les x qu'il veut en temps $O(1)$ [F est une "boîte noire"]

- $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ ssi une fonction pseudo-aléatoire
  $(k, x) \mapsto F_k(x)$

si $\forall D$ APP, $\left| \Pr_k[D^{F_k}(1^n) = 1] - \Pr_f[D^f(1^n) = 1] \right| \leq \text{negl}(n)$

k : unif. $\in \{0,1\}^n$; f : unif dans $\{0,1\}^n \to \{0,1\}^n$

Preuve pour CTR

- $m = m^1 \| m^2 \| \dots \| m^t \rightsquigarrow c^i = m^i \oplus F_k(IV \| i)$
- On définit $\widetilde{Enc}_f(m)$ par $c^i = m^i \oplus f(IV \| i)$ où f uniforme parmi $\{0,1\}^n \to \{0,1\}^n$
  ↳ $\widetilde{Exp}$

Lemme $\left| Pr[Exp(n)=1] - Pr[\widetilde{Exp}(n)=1] \right| \leq negl(n)$.

Si c'était pas le cas, on aurait un distinguer pour F_k. □

- On montre que $Pr[\widetilde{Exp}(n)=1] \leq 1/2 + negl(n)$
  - × A_0 appelle f plusieurs fois → à chaque fois IV est tiré uniformément.
    Si tous les IV sont différents → $f(IV\|1), f(IV\|2), \dots$ sont aléatoires uniformes
    ⇒ le chiffrement est équivalent à Vernam → $Pr[\widetilde{Exp}(n)=1] = 1/2$

Preuve pour CTR

$$\times \quad \Pr[2 \text{ IV soient égaux}] \leq \frac{\#\text{appels}}{2^{|IV|}} \leq \frac{poly(n)}{exp(n)} \leq negl(n)$$

$$\Pr\left[\widetilde{Exp}(n)=1\right] = \Pr\left[\widetilde{Exp}(n)=1 \mid \text{les IV sont distincts}\right] \Pr[\text{IV sont distincts}]$$

($\Pr[\widetilde{Exp}(n)=1 \mid \text{les IV sont distincts}] = 1/2$, $\Pr[\text{IV sont distincts}] \leq 1$)

$$+ \Pr\left[\widetilde{Exp}(n)=1 \mid 2 \text{ IV sont égaux}\right] \Pr[2 \text{ IV sont égaux}]$$

($\Pr[\widetilde{Exp}(n)=1 \mid 2 \text{ IV sont égaux}] \leq 1$, $\Pr[2 \text{ IV sont égaux}] \leq negl(n)$)

$$\leq 1/2 + negl(n)$$

Conclusion

- Deux grands types de constructions pratiques :
  - Chiffrement par flot
  - Chiffrement par blocs
- Constructions souvent alambiquées $\rightarrow$ justifications hors du cadre de ce cours
- Briques de base sur lesquelles on construit des protocoles complexes :
  - Théorie : reposent sur des conjectures de théorie de la complexité
  - Pratique : constructions heuristiques, très testées