Séance 5 - Travaux Dirigés
Chiffrements par bloc

Yann Rotella

2026

Seul.e 45 minutes

Exercice 1. *Le critère d'avalanche.*
Le critère d'avalanche (avalanche criterion) est un premier critère à prendre en compte pour fixer le nombre de tours d'un chiffrement de type SPN.

Soit n un entier et soit F une fonction de $\{0,1\}^n$ dans $\{0,1\}^n$. On note $f_1, \ldots, f_n$ les fonctions *coordonnées* de f.

Définition 1. *(Fonctions coordonnées). Soient n et m deux entiers. Pour toute fonction $F : \{0,1\}^n \to \{0,1\}^m$, on appelle fonction coordonée de F toute fonction $f_i : \{0,1\}^n \to \{0,1\}$ pour $0 \leq i \leq m-1$ définie par*

$$x \mapsto f_i(x) = (F(x))_i$$

où $(F(x))_i$ est le i-ème bit dans la représentation binaire de $F(x)$.

On suppose maintenant que chaque $f_i(x)$ n'a besoin que de ℓ_i bits de x pour être calculée.
On note alors

$$\ell = \max_{0 \leq i \leq n-1} \ell_i = \text{Avalanche}(F)$$

(1) Rappeler les deux critères nécessaires vus en cours qui doivent garantir la sécurité d'un chiffrement par bloc.

(2) Lequel de ces deux critères essayons-nous de capturer ici ?

(3) En supposant une construction de type SPN (comme proposée par Claude Shannon), avec des boîtes-S de 6 bits et des permutations des fils, que vaut ℓ pour la fonction de tour (sans ajout de clef) ?

(4) Soient $F : \{0,1\}^n \to \{0,1\}^n$ et $G : \{0,1\}^n \to \{0,1\}^n$. On note $\ell_F = \text{Avalanche}(F)$ et $\ell_G = \text{Avalanche}(G)$. Quelle borne pouvez-vous donner sur $\text{Avalanche}(F \circ G)$? Montrer la.

(5) Soit n un entier et un SPN « à la Shannon » avec des boîtes-S opérant sur 4 bits, combien de tours faut-il faire *au minimum* ? Justifier avec un critère du cours.

(6) Est-ce suffisant ? Justifier (peut-être avec un exemple ?)

En groupe - à vous de jouer

Exercice 2. *SPN dernier tour.*
On considère un SPN « général », i.e. soit

$$\mathcal{L} : \{0,1\}^n \to \{0,1\}^n$$

une opération linéaire et soit

$$\mathcal{S} : \{0,1\}^n \to \{0,1\}^n$$

une concaténation de boîte-S et k une clef secrète. On ne détaille pas le cadencement de clefs.

On considère alors le chiffrement par bloc suivant.

$$R_i = \mathcal{L} \circ \mathcal{S} \circ \mathrm{Add}_{k_i}$$

(1) Montrer qu'au niveau de la sécurité, et indépendamment du nombre de tours, les deux dernières opérations sont inutiles.

(2) Soit r le nombre de tours. En supposant $k_r, k_{r-1}, \ldots, k_1$ uniformément distribuées et indépendantes, l'avant dernière couche linéaire est aussi inutile du point de vue de la sécurité.

On regarde maintenant un SPN particulier « à la »Shannon. Et on suppose qu'au tour $r-1$, on identifie qu'un bit en sortie de chaque boîte-S ne dépend pas de tous les bits en entrée mais que c'est le cas au tour r.

(3) Décrire un schéma d'attaque sur un tel chiffrement qui retrouve toute la clef.

(4) Donner sa complexité en fonction de paramètres que vous choisissez.

(5) Essayez d'aller plus loin en supposant par exemple que la taille des boîtes-S est petite (4 bits). Expliquer quand nous n'avons pas de PRP.

Exercice 3. *Schémas de Feistel - combien de tours ?.*
La construction de type Feistel est une construction qui permet de construire une fonction sur $2n$ bits, bijective à partir de n'importe quelle fonction de n bits vers n bits. Pour toute fonction $F : \{0,1\}^n \to \{0,1\}^n$, on note $\mathrm{Fesitel}[F] : \{0,1\}^{2n} \to \{0,1\}^{2n}$ la fonction définie par

$$X = X_L || X_R \mapsto Y = \mathrm{Fesitel}[F](X) = X_R || (F(X_R) \oplus X_L)$$

(1) Dessiner le schéma de la construction Feistel.

(2) Montrer que, peu importe la fonction F (bijective, injective ou surjective), la construction en Feistel qui en résulte, i.e. l'application $\mathrm{Fesitel}[F]$ est bijective. Donner alors sa fonction inverse.

Maintenant on suppose que F est choisie dans $\mathcal{F}$ une PRF, c'est-à-dire que $\mathcal{F}$ est une famille de fonction (indistinguable de fonctions aléatoires), paramétrée par une clef k. On choisit alors de regarder l'itération successive d'un schéma de Feistel pour un certain nombre de tours. L'objectif reste toujours de construire une PRP.

(3) Dessiner le schéma pour 1, 2 et 3 tours en faisant bien tout apparaître.

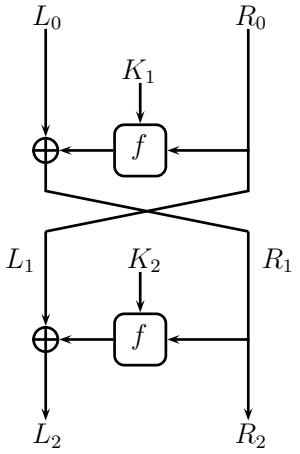
(4) Montrer que 1 tour de Feistel n'est pas une PRP. Donner la complexité ou l'estimation de l'avantage.

(5) Montrer que 2 tours de Feistel n'est pas une PRP. Donner la complexité ou l'estimation de l'avantage.

(6) En exploitant un modèle plus fort de l'attaquant pour distinguer $\mathrm{Fesitel}[F]$ d'une permutation aléatoire, attaquer 3 tours, donner la complexité.

Exercices complémentaires

Exercice 4. *Application directe Feistel à la main.*
Le réseau de Feistel de la figure suivante travaille sur un état de 8 bits :



La fonction f prend en entrée une sous-clé de 4 bits K_{i+1} et une donnée de 4 bits R_i, additionne bit-à-bit les deux entrées et applique au résultat une couche de confusion et ensuite une couche de diffusion :

$$\begin{aligned} f : \{0,1\}^4 \times \{0,1\}^4 &\rightarrow \{0,1\}^4 \\ f(K_{i+1}, R_i) &= P(S(K_{i+1} \oplus R_i)). \end{aligned}$$

où S est une boîte-S donnée par la table suivante :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2

et $P : \{0,1\}^4 \rightarrow \{0,1\}^4$ une permutation bit-à-bit donnée par

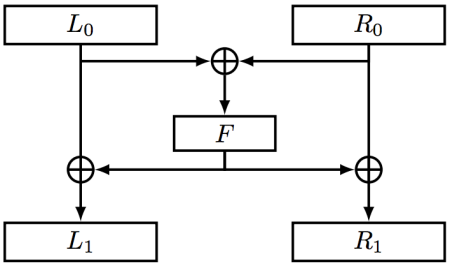
$$P = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

(1) Chiffrer le message $m = 163_{10} = 1010\,0011_2$ avec les sous-clés $K_1 = 7$ est $K_2 = 12$. On notera le chiffré $c = (L_2|R_2)$. On considère que les bits de poids faible sont à droite.

(2) Faire un dessin de l'algorithme de déchiffrement. Expliquer son fonctionnement. Est-il nécessaire que la fonction f soit inversible ?

Exercice 5. *IDEA.*
IDEA (*International Data Encryption Algorithm*) est un chiffrement symétrique par bloc, originellement présenté en 1990. Il emploie des clés de 128 bits pour chiffrer des bloc de 64 bits.

Le schéma IDEA est basé sur une variante du mécanisme de Feistel, dont la fonction de tour (on ignore ici l'addition des sous-clés) est décrite ci-dessous :



(1) On se concentre pour l'instant sur la fonction de chiffrement n'ayant qu'un tour. Écrire les équations donnant l'expression du chiffré (L_1, R_1) en fonction du clair (L_0, R_0).

(2) Montrer que ce schéma (on ne considère toujours qu'un tour) est inversible quelle que soit la fonction F et donner les formules décrivant le déchiffrement.

(3) Décrire un schéma de Feistel à trois tours (sans la permutation finale des deux bloc L_3 et R_3) qui lui est équivalent.

(4) Montrer comment distinguer la fonction de chiffrement $(L_0, R_0) \mapsto (L_1, R_1)$ d'une transformation aléatoire.

(5) Même question si l'on empile plusieurs tours de chiffrement (par exemple, si on considère la fonction $(L_0, R_0) \mapsto (L_2, R_2)$ avec la même fonction F.

Exercice 6.

La non-linéarité est nécessaire Considérons un système de chiffrement par bloc qui suit le schéma de Feistel et dont la fonction f utilisée à chaque tour est constituée d'une transformation linéaire A, suivie d'une addition bit à bit avec la clé k, puis d'une seconde transformation linéaire B

$$f(x) = B(A(x) \oplus k).$$

Montrer comment il est possible d'attaquer un tel système.