Cryptanalyse

Cours 6 - Cryptanalyse Linéaire

Maxime Bombar

Mardi 08 Septembre 2024

Rappels de la Semaine Dernière

Attaque Statistique

- Une attaque statistique cherche à exploiter des relations qui existent entre le chiffré et le message avec une certaine probabilité afin de retrouver de l'information sur la clé secrète.

- Une telle attaque repose en général sur un **distingueur** entre un chiffrement E_k et une **permutation aléatoire**.

Attaque de dernier tour

$$E_k = F_{k_r} \circ \cdots \circ F_{k_1}$$

On suppose que l'on a un distingueur $\mathscr{D}$ pour $G_k \stackrel{\text{def}}{=} F_{k_{r-1}} \circ \cdots \circ F_{k_1}$.

Wrong-Key Randomization Hypothesis : Si $\mathbf{c} = E_k(\mathbf{m})$ alors $F_{k_r}(\mathbf{c}) = G_k(\mathbf{m})$ mais si $k' \neq k_r$ alors $F_{k'}$ se comporte comme une permutation aléatoire.

- Pour tout candidat k_r on cherche à observer la relation sur $(\mathbf{m}, F_{k_r}(\mathbf{c}))$ pour **plein** de couples $(\mathbf{m}, \mathbf{c})$, clairs-chiffrés.
- Si on observe la relation, on incrémente un compteur pour k_r.
- On renvoie le candidat avec le plus gros compteur.

A un intérêt VS recherche exhaustive si on peut **décimer** l'espace de recherche de k_r.

$$\begin{tikzcd}
\Delta\mathbf{m} = \mathbf{m} \oplus \mathbf{m}' = \alpha \arrow[d] & \\
\boxed{E} \arrow[d] & k \arrow[l] \\
\Delta\mathbf{c} = \mathbf{c} \oplus \mathbf{c}' = \beta &
\end{tikzcd}$$

- On cherche (α, β) telle que la différentielle $(\alpha \to \beta)$ se produise avec bonne probabilité.
- Une différentielle est **inchangée** par **addition de clé**.
- On étudie le chiffrement au niveau des boîtes S.

Tabulation de la distribution des Différentielles

Pour chaque boîte S, et pour chaque paire (α, β), on peut **précalculer**

$$\mathrm{DDT}[\alpha][\beta] = \#\{\mathbf{x} \mid S(\mathbf{x}) + S(\mathbf{x} + \alpha) = \beta\}.$$

Si $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ alors la **probabilité** d'observer une différentielle $(\alpha \to \beta)$ pour un message $\mathbf{m}$ tiré uniformément est

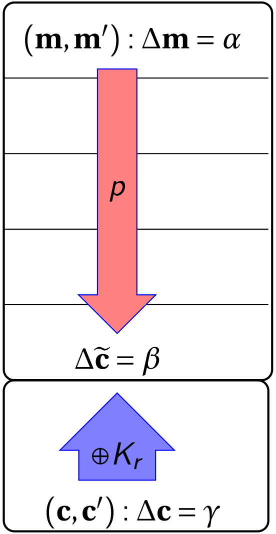
$$\mathbb{P}_{\mathbf{m}}\Big(S(\mathbf{m}) + S(\mathbf{m} + \alpha) = \beta\Big) = \frac{\mathrm{DDT}[\alpha][\beta]}{2^n}.$$

Trace Différentielle

Pour prendre en compte plusieurs tours, on **compose** les différentielles.

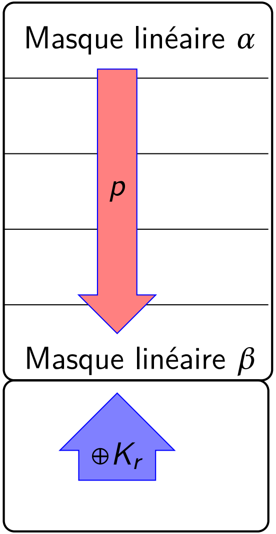
Differential characteristic

- $(\alpha_0 \to \alpha_1 \to \cdots \to \alpha_r)$ telle que $(\alpha_{i-1} \to \alpha_i)$ soit une différentielle pour le tour i.
- La probabilité d'une trace est le produit des probabilités de chaque sous-différentielle (**hypothèse d'indépendance des tours**).
- La probabilité d'une différentielle $(\alpha_0 \to \alpha_r)$ sur l'ensemble du chiffré est **minorée** par la probabilité de n'importe quelle trace : attention aux effets de **clustering** (pour les concepteurs de chiffrement).
- Les couches de diffusion (couches linéaires) perturbent l'étude en augmentant les traces possibles.



- Attaque par **clairs choisis** de différence α telle que $(\alpha \mapsto_{r-1} \beta)$ avec proba $p >> 2^{-|\text{taille de bloc}|}$
- On calcule $\Theta(1/p)$ couples $[(\mathbf{m},\mathbf{m}'),(\mathbf{c},\mathbf{c}')]$
- On caractérise un **petit** ensemble de candidats k_r.
- Pour **chaque candidat**, on inverse le dernier tour pour **chaque paire** (clairs-chiffrés), et on espère observer la différentielle (distingueur).

Aujourd'hui : Cryptanalyse Linéaire



- Nouveau type d'**attaque statistique**.
- Rend possible des attaques à **clairs connus**.
- Cadre **similaire** à la cryptanalyse différentielle.

Introduction et principes

Historique

- Cryptanalyse à **clairs connus**.
- Initiée par H. Gilbert, G. Chassé et A. Tardy-Corfdir en 1991 pour la cryptanalyse de FEAL.
- Formalisée par Matsui en 1993.
- A permis la **première** cryptanalyse de DES, avec 2^{47} couples clairs-chiffrés.

Idée

- On cherche une relation **linéaire** reliant clair, chiffré et clé avec bonne probabilité.
- On utilise cette relation comme un **distingueur**.

Gilbert, Chassé - *A Statistical Attack of the FEAL-8 Cryptosystem*, 1990
Tardy-Cofdir, Gilbert - *A known plaintext attack of FEAL-4 and FEAL-6*, 1991
Matsui - *Linear Cryptanalysis Method for DES Cipher*, 1993.

Le cas typique idéal

Une remarque utile

Soient E, F deux ensembles finis et soit $f : E \to F$. Soit X une variable aléatoire uniforme sur E.

- Si f est **bijective**, alors $f(X)$ est uniforme sur F.
- Si E, F sont deux espaces vectoriels sur $\mathbb{F}_q$, et si f est **linéaire surjective**, alors $f(X)$ est uniforme sur F.

E_k est une permutation sur n bits, donc $\mathbf{c} \stackrel{\text{def}}{=} E_k(\mathbf{m})$ est uniforme sur $\mathbb{F}_2^n$ pour un message uniforme $\mathbf{m} \leftarrow \mathbb{F}_2^n$. Si $\mathbf{m}$ et $\mathbf{c}$ étaient décorrélés, alors pour toutes formes linéaires non nulles $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$, on devrait avoir

$$\mathbb{P}_{\mathbf{m}}\Big[f(\mathbf{m}) = g(E_k(\mathbf{m}))\Big] = \frac{1}{2}.$$

Distingueur Linéaire

On appelle distingueur linéaire de biais $\varepsilon > 0$ une paire (f, g) de formes linéaires non nulles telles que

$$\mathbb{P}_{\mathbf{m}}\Big[f(\mathbf{m}) = g(E_k(\mathbf{m}))\Big] = \frac{1}{2}\Big(1 \pm \varepsilon\Big).$$

Masques linéaires

Un distingueur linéaire est représenté par une paire $(\alpha, \beta) \in \left(\mathbb{F}_2^n \setminus \{0\}\right)^2$ telle que

$$\mathbb{P}_{\mathbf{m}}\Big[\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{c} \rangle = 0\Big] = \frac{1}{2}\Big(1 \pm \varepsilon\Big).$$

Principe de la cryptanalyse linéaire

$$E_k = F_{k_r} \circ \underbrace{F_{k_{r-1}} \cdots \circ F_{k_1}}_{\overset{\text{def}}{=} G_k}$$

Plus généralement, on cherche $(\alpha, \beta, \gamma) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^\kappa$ tel que

$$\mathbb{P}_{\mathbf{m}}\Big[\langle \alpha, \mathbf{m} \rangle + \langle \beta, G_k(\mathbf{m}) \rangle + \langle \gamma, k_r \rangle = 0\Big] = \frac{1}{2}\Big(1 \pm \varepsilon\Big).$$

Le nombre de couples $(\mathbf{m}, \mathbf{c})$ dont on a besoin pour distinguer G_k d'une permutation aléatoire à l'aide de cette relation est **au-moins** $\Omega\left(\frac{1}{\varepsilon^2}\right)$.

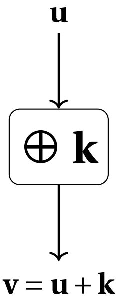
Boîtes S actives

Comme pour la cryptanalyse différentielle, on veut restreindre l'espace de recherche pour k_r.

On appelle boîte S **active**, une boîte S du dernier tour dont au-moins un bit d'entrée intervient dans l'équation linéaire.

Propagation d'une relation linéaire : Cas des ajouts de clé

$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle = 0$$
avec probabilité $\frac{1}{2}(1+\varepsilon)$

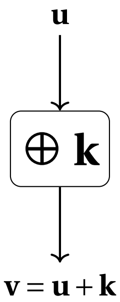


$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = \langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle + \langle \beta, \mathbf{k} \rangle$

- Si $\langle \beta, \mathbf{k} \rangle = 0$ alors $\mathbb{P}_{\mathbf{m}}\Big(\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = 0\Big) = \frac{1}{2}(1+\varepsilon)$
- Si $\langle \beta, \mathbf{k} \rangle = 1$ alors $\mathbb{P}_{\mathbf{m}}\Big(\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = 0\Big) = \frac{1}{2}(1-\varepsilon)$

Propagation d'une relation linéaire : Cas des ajouts de clé

$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle = 0$$
avec probabilité $\dfrac{1}{2}(1+\varepsilon)$



$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = \langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle + \langle \beta, \mathbf{k} \rangle$$

- Si $\langle \beta, \mathbf{k} \rangle = 0$ alors $\mathbb{P}_{\mathbf{m}}\Big(\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = 0\Big) = \dfrac{1}{2}(1+\varepsilon)$
- Si $\langle \beta, \mathbf{k} \rangle = 1$ alors $\mathbb{P}_{\mathbf{m}}\Big(\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = 0\Big) = \dfrac{1}{2}(1-\varepsilon)$

$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{v} \rangle = 0$$
avec probabilité $\dfrac{1}{2}(1\pm\varepsilon)$

Propagation d'une relation linéaire : Étape de diffusion

$$\mathbf{u}$$

$$\downarrow$$

Permutation linéaire P

$$\downarrow$$

$$\mathbf{v} = P(\mathbf{u})$$

$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle = 0$$

avec probabilité $\frac{1}{2}(1+\varepsilon)$

$$\langle \beta, \mathbf{u} \rangle = \langle P(\beta), P(\mathbf{u}) \rangle = \langle P(\beta), \mathbf{v} \rangle$$

Propagation d'une relation linéaire : Étape de diffusion

$$\mathbf{u} \longrightarrow \boxed{\text{Permutation linéaire } P} \longrightarrow \mathbf{v} = P(\mathbf{u})$$

$$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle = 0$$

avec probabilité $\frac{1}{2}(1+\varepsilon)$

$$\langle \beta, \mathbf{u} \rangle = \langle P(\beta), P(\mathbf{u}) \rangle = \langle P(\beta), \mathbf{v} \rangle$$

$$\langle \alpha, \mathbf{m} \rangle + \langle P(\beta), \mathbf{v} \rangle = 0$$

avec probabilité $\frac{1}{2}(1+\varepsilon)$

Propagation d'une relation linéaire : Boîtes S

$\mathbf{u}$

Fonction booléenne non-linéaire S

$\mathbf{v} = S(\mathbf{u})$

$\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{u} \rangle = 0$

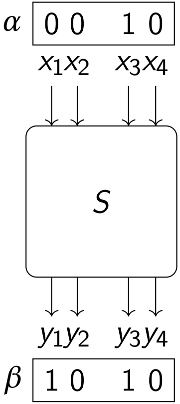
avec probabilité $\frac{1}{2}(1+\varepsilon)$

?

Approximation linéaires

Un exemple

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	4	f	2	d	5	b	7	3	9	1	0	8	a	e	6	c



$\mathbf{x}$	$\mathbf{y}$	$x_3 = y_1 + y_3$?
(0, 0, 0, 0)	(0, 1, 0, 0)	✓
(0, 0, 0, 1)	(1, 1, 1, 1)	✓
(0, 0, 1, 0)	(0, 0, 1, 0)	✓
(0, 0, 1, 1)	(1, 1, 0, 1)	✓
(0, 1, 0, 0)	(0, 1, 0, 1)	✓
(0, 1, 0, 1)	(1, 0, 1, 1)	✓
(0, 1, 1, 0)	(0, 1, 1, 1)	✓
(0, 1, 1, 1)	(0, 0, 1, 1)	✓

$\mathbf{x}$	$\mathbf{y}$	$x_3 = y_1 + y_3$?
(1, 0, 0, 0)	(1, 0, 0, 1)	✗
(1, 0, 0, 1)	(0, 0, 0, 1)	✓
(1, 0, 1, 0)	(0, 0, 0, 0)	✗
(1, 0, 1, 1)	(1, 0, 0, 0)	✓
(1, 1, 0, 0)	(1, 0, 1, 0)	✓
(1, 1, 0, 1)	(1, 1, 1, 0)	✓
(1, 1, 1, 0)	(0, 1, 1, 0)	✓
(1, 1, 1, 1)	(1, 1, 0, 0)	✓

$\langle \alpha, \mathbf{x} \rangle + \langle \beta, S(\mathbf{x}) \rangle = 0$ pour 14 entrées sur 16.

Qualité d'une Approximation Linéaire

On mesure la qualité d'une approximation linéaire (α, β) d'une boîte S sur n bits par les métriques suivantes :

- **Nombre de Solutions :** $\sigma_{\alpha,\beta} = \#\{\mathbf{x} \mid \langle \alpha, \mathbf{x} \rangle + \langle \beta, S(\mathbf{x}) \rangle = 0\}$
- **Probabilité :** $p_{\alpha,\beta} = \dfrac{\sigma_{\alpha,\beta}}{2^n}$
- **Biais :** $\varepsilon_{\alpha,\beta}$ $\quad p_{\alpha,\beta} = \dfrac{1}{2}(1 + \varepsilon_{\alpha,\beta})$ *i.e.*, $\varepsilon_{\alpha,\beta} = 2p_{\alpha,\beta} - 1$

- Si $\varepsilon_{\alpha,\beta} = 0$, on n'apprend **rien**.
- Si $\varepsilon_{\alpha,\beta} > 0$, alors $\langle \alpha, \mathbf{x} \rangle = \langle \beta, S(\mathbf{x}) \rangle$ est une **bonne approximation**.
- Si $\varepsilon_{\alpha,\beta} < 0$, alors $\langle \alpha, \mathbf{x} \rangle \oplus 1 = \langle \beta, S(\mathbf{x}) \rangle$ est une **bonne approximation**.

Table des Approximations Linéaires (LAT)

Pour chaque masque (α, β), on représente souvent l'écart du nombre de solutions par rapport à la moitié dans une table :

$$LAT[\alpha][\beta] = \sigma_{\alpha,\beta} - 2^{n-1} = 2^{n-1}\varepsilon_{\alpha,\beta}.$$

LAT de l'exemple précédent

$\alpha \setminus \beta$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	2	-	-2	-	2	-	-2	4	2	-	2	-4	2	-	2
2	-	-2	-	-2	-	-2	-	-2	-2	-	**6**	-	-2	-	-2	-
3	-	-	4	-	-	-	-4	-	-2	-2	-2	2	-2	-2	-2	2
4	-	-	4	-	2	2	2	-2	-	4	-	-	2	-2	-2	-2
5	-	2	-	2	2	-4	-2	-	-	2	-	2	2	4	-2	-
6	-	-2	-	2	-2	-4	2	-4	2	-	-2	-	-	-2	-	2
7	-	-	-	-	-2	-2	2	2	-2	2	-2	2	-4	-	-	-4
8	-	-4	-2	2	-2	2	-4	-	2	2	-	-	-	-	-2	-2
9	-	2	2	-	-2	-	-	-2	2	-4	-	-2	-	2	-2	-4
a	-	2	2	4	-2	-	-	2	-	2	2	-4	-2	-	-	2
b	-	-	2	-2	-2	-2	-	4	4	-	2	2	2	-2	-	-
c	-	4	-2	-2	-4	-	-2	-2	-2	2	-	-	2	-2	-	-
d	-	2	-2	-	4	-2	-2	-	2	-	-	-2	-2	-4	-	-2
e	-	2	-2	4	-	2	2	-	-	-2	2	4	-	-2	-2	-
f	-	-	2	2	-	-	-2	-2	-	-	2	2	-	-	**6**	-2

On retrouve que $\alpha = (0,0,1,0)$ et $\beta = (1,0,1,0)$ nous offrent **une bonne approximation**.

Chaîner les Approximations Linéaires

Linear Characteristics

Pour trouver une bonne approximation linéaire de plusieurs tours du chiffrement, on va chercher des bonnes approximations successives (α_i, β_i) telles que $\alpha_{i+1} = \beta_i$. La qualité d'une trace linéaire est donnée par le lemme suivant.

Le *Piling-Up* Lemma

Soient $X_1, \ldots, X_m$ m variables aléatoires **indépendantes**, à valeurs dans $\mathbb{F}_2$. Pour tout i, on note ε_i leur biais :

$$\mathbb{P}(X_i = 0) = \frac{1}{2}(1 + \varepsilon_i).$$

Alors

$$\mathbb{P}(X_1 + \cdots + X_m = 0) = \frac{1}{2}\left(1 + \prod_i \varepsilon_i\right).$$

En Pratique

Le *Piling-Up* Lemma

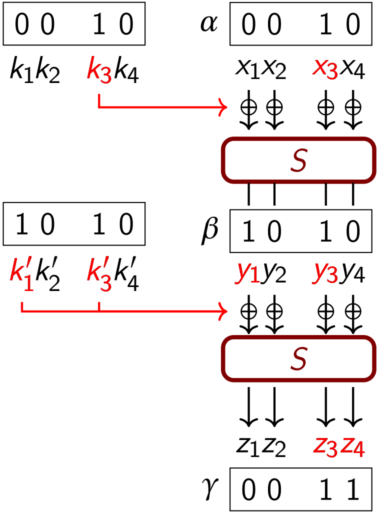
Soient $X_1, \ldots, X_m$ m variables aléatoires **indépendantes**, à valeurs dans $\mathbb{F}_2$. Pour tout i, on note ε_i leur biais :

$$\mathbb{P}(X_i = 0) = \frac{1}{2}(1 + \varepsilon_i).$$

Alors

$$\mathbb{P}(X_1 + \cdots + X_m = 0) = \frac{1}{2}\Big(1 + \prod_i \varepsilon_i\Big).$$

On va chercher une trace linéaire $(\alpha_0, \ldots, \alpha_r)$ qui maximise $\left|\prod_i \varepsilon_i\right|$.



Approximations Linéaires :

$$\langle \alpha, \mathbf{x} \rangle + \langle \alpha, \mathbf{k} \rangle + \langle \beta, \mathbf{y} \rangle = 0$$
$$x_3 + k_3 = y_1 + y_3$$

(Eq1)

$$\langle \beta, \mathbf{y} \rangle + \langle \beta, \mathbf{k}' \rangle + \langle \gamma, \mathbf{z} \rangle = 0$$
$$y_1 + y_3 + k'_1 + k'_3 = z_3 + z_4$$

(Eq2)

$$\langle \alpha, \mathbf{x} \rangle + \langle (\alpha, \beta), (\mathbf{k}, \mathbf{k}') \rangle + \langle \gamma, \mathbf{z} \rangle = 0$$

(Eq3)

Exemple (Suite)

- **(Eq1) :** $\langle \alpha, \mathbf{x} \rangle + \langle \alpha, \mathbf{k} \rangle + \langle \beta, \mathbf{y} \rangle = 0$ a pour biais $\dfrac{\mathrm{LAT}[2][10]}{2^3} = \dfrac{6}{8} = \dfrac{3}{4}$.
- **(Eq2) :** $\langle \beta, \mathbf{y} \rangle + \langle \beta, \mathbf{k}' \rangle + \langle \gamma, \mathbf{z} \rangle = 0$ a pour biais $\dfrac{\mathrm{LAT}[10][3]}{2^3} = \dfrac{4}{8} = \dfrac{1}{2}$.
- Donc **(Eq3)** a pour biais $\dfrac{3}{4} \times \dfrac{1}{2} = \dfrac{3}{8}$. Autrement dit :

$$\mathbb{P}_{\mathbf{x}}\left(\langle \alpha, \mathbf{x} \rangle + \langle (\alpha, \beta), (\mathbf{k}, \mathbf{k}') \rangle + \langle \gamma, \mathbf{z} \rangle = 0\right) = \frac{1}{2}\left(1 + \frac{3}{8}\right).$$

Retrouver la clé secrète

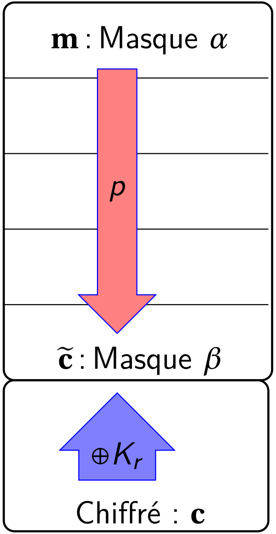
Cryptanalyse Linéaire Complète

On suppose que l'on a une approximation $\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{c} \rangle + \langle \gamma, \mathbf{k} \rangle = 0$ avec biais ε.

- On récupère $\Omega(1/\varepsilon^2)$ couples (clair, chiffré) $(\mathbf{m}, \mathbf{c})$.
- On initialise deux compteurs C_0 et C_1.
- Pour chaque couple $(\mathbf{m}, \mathbf{c})$
  - Si $\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{c} \rangle = 0$, on incrémente C_0.
  - Si $\langle \alpha, \mathbf{m} \rangle + \langle \beta, \mathbf{c} \rangle = 1$, on incrémente C_1.
- Si $C_0 > C_1$ on conclut que $\langle \gamma, \mathbf{k} \rangle = 0$.
- Si $C_1 > C_0$ on conclut que $\langle \gamma, \mathbf{k} \rangle = 1$.

- Cet algorithme nous fournit 1 equation linéaire sur $\mathbf{k}$.
- Si $\mathbf{k}$ est sur m bits, on va en chercher m **linéairement indépendantes**.
- ⚠ Nécessite une approximation des r tours du chiffrement.

Attaque sur le Dernier Tour



- On trouve une approximation linéaire (α, β)

pour le chiffré réduit à $r-1$ tours, de proba $\frac{1}{2}(1+\varepsilon)$.

- On récupère $\Omega(1/\varepsilon^2)$ couples (clair, chiffré) $(\mathbf{m}, \mathbf{c})$.
- Pour chaque candidat k_r :
  - On initialise deux compteurs $C_+ = 0$ et $C_- = 0$.
  - Pour chaque $\mathbf{c}$:
    - On inverse un tour de chiffrement : $\mathbf{c} \mapsto \widetilde{\mathbf{c}}$.
    - Si $\langle \alpha, \mathbf{m} \rangle + \langle \beta, \widetilde{\mathbf{c}} \rangle = 0$, on incrémente C_+.
    - Sinon on incrémente C_-.

La bonne clé doit avoir une grosse différence $|C_+ - C_-|$.

The Hull Effect

- En général, on estime le biais d'une approximation (α, β) à l'aide d'une unique trace $(\alpha = \alpha_0, \ldots, \alpha_r = \beta)$.
- Cependant, le vrai biais dépend de **toutes** les traces compatibles.
- Il peut-être en réalité **plus faible** que le biais d'une trace particulière, s'il existe plusieurs traces avec des biais de signes opposés qui peuvent voir leurs effets s'annuler.
- En pratique, les attaques peuvent être **moins efficaces** que prédites dans la théorie.

Nyberg - *Linear Approximation of Block Ciphers*, EUROCRYPT 1994

Contre-Mesures

Objectif du Concepteur

Biais d'une fonction booléenne

Soit $f : \mathbb{F}_2^n \to \mathbb{F}_2$ une fonction booléenne en n variables. Son biais est

$$\mathscr{E}(f) \stackrel{\text{def}}{=} \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = 2^n - 2w(f).$$

Pour étudier la résistance d'une boîte $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$, on cherche à calculer les biais de toutes les fonctions booléennes de la forme :

$$x \mapsto \langle \alpha, x \rangle + \langle \beta, S(x) \rangle$$

pour $(\alpha, \beta) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \setminus \{0\}$.

Transformée de Fourier

Soit $f : \mathbb{F}_2^n \to \mathbb{F}_2$ une fonction booléenne en n variables. Sa transformée de Fourier (ou transformée de Walsh) est

$$\widehat{f} : \left\{ \begin{array}{ccc} \mathbb{F}_2^n & \longrightarrow & \mathbb{Z} \\ \alpha & \longmapsto & \mathscr{E}\Big[x \mapsto f(x) + \langle \alpha, x \rangle\Big] = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle \alpha, x \rangle} \end{array} \right.$$

Concept de Linéarité

Soit $f : \mathbb{F}_2^n \to \mathbb{F}_2$ une fonction booléenne en n variables. On définit sa **linéarité** comme son plus gros coefficient de Fourier :

$$\mathscr{L}(f) \overset{\text{def}}{=} \max_{\alpha \in \mathbb{F}_2^n} \left| \widehat{f}(\alpha) \right|.$$

Soit $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ une boîte S sur n bits. Sa linéarité est par définition la plus grande linéarité parmi toutes les fonctions booléennes $S_\beta \overset{\text{def}}{=} x \mapsto \langle \beta, S(x) \rangle$:

$$\mathscr{L}(S) \overset{\text{def}}{=} \max_{\beta \in \mathbb{F}_2^n \setminus \{0\}} \mathscr{L}(S_\beta) = \max_{\alpha, \beta} \mathscr{E}\left[x \mapsto \langle \alpha, x \rangle + \langle \beta, S(x) \rangle \right].$$

Résistance à la Cryptanalyse Linéaire

Un chiffrement par blocs est d'autant plus résistant aux attaques linéaires que ses boîtes S ont une petite linéarité.

Pour n pair, on ne connaît pas de borne inférieure pour la linéarité d'une boîte $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$. La plus petite linéarité connue pour le moment est

$$\mathscr{L}(S) = 2^{\frac{n}{2}+1}.$$

L'AES

La boîte S de l'AES (qui représente l'inversion de $\mathbb{F}_{2^8}$ avec $0 \mapsto 0$) atteint cette valeur minimale connue.