S-Boxes à bas coût par des réseaux Feistel et MISTY

A. Canteaut, S. Duval, G. Leurent

Inria

03/12/2015

Table des Matières

1. Introduction
2. Paramètres de sécurité
3. Feistel et MISTY à clé fixée
4. Construction
5. Conclusion

Le contexte : le chiffrement symétrique

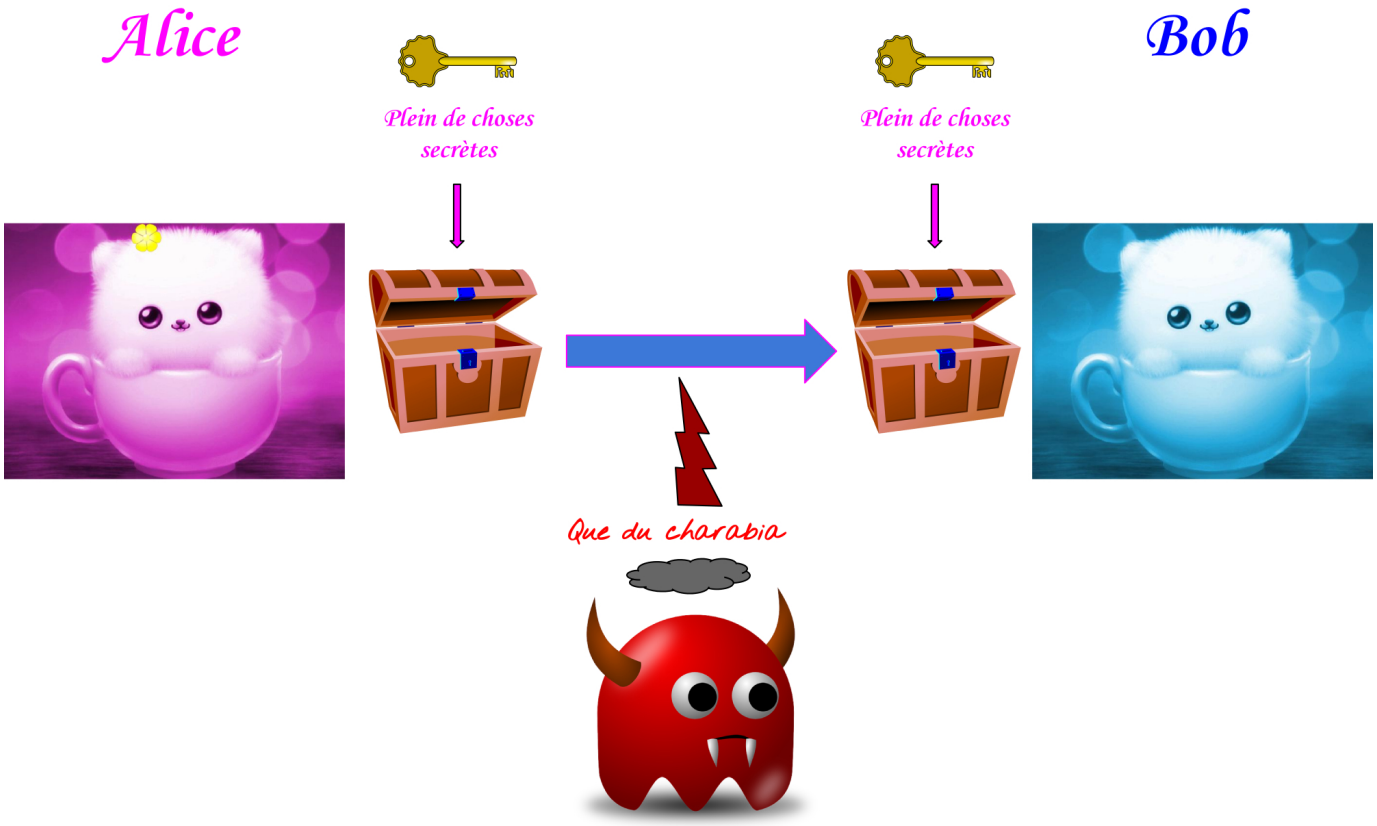
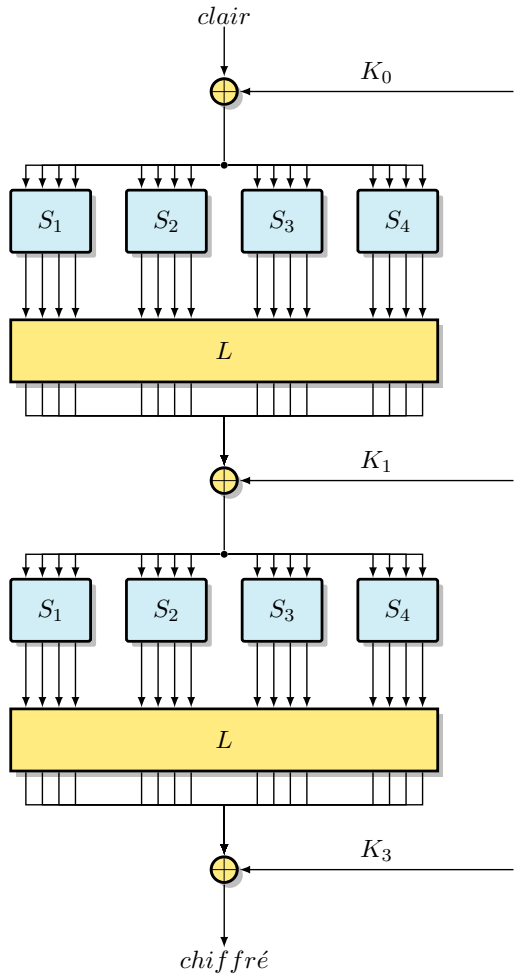


Schéma d'un chiffrement symétrique

Les chiffrements par blocs

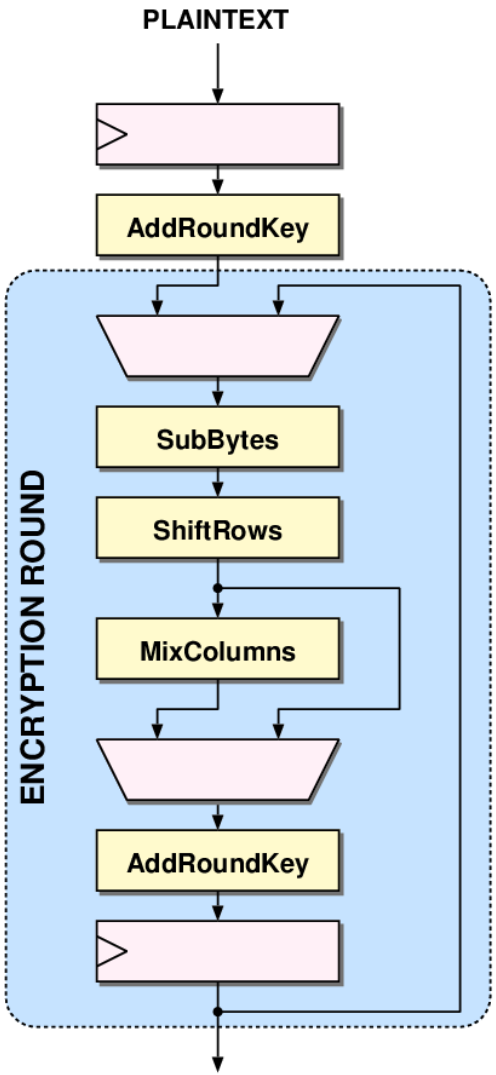
Critères de Shannon

1. Diffusion
   - Chaque bit de l'entrée doit affecter tous les bits de sortie
   - On utilise généralement des fonctions linéaires
2. Confusion
   - La relation entre le texte clair et le texte chiffré doit être difficile à trouver
   - Cela nécessite des fonctions non-linéaires
   - Ces fonctions sont souvent implémentées en tables : S-Boxes



Chiffrement SPN

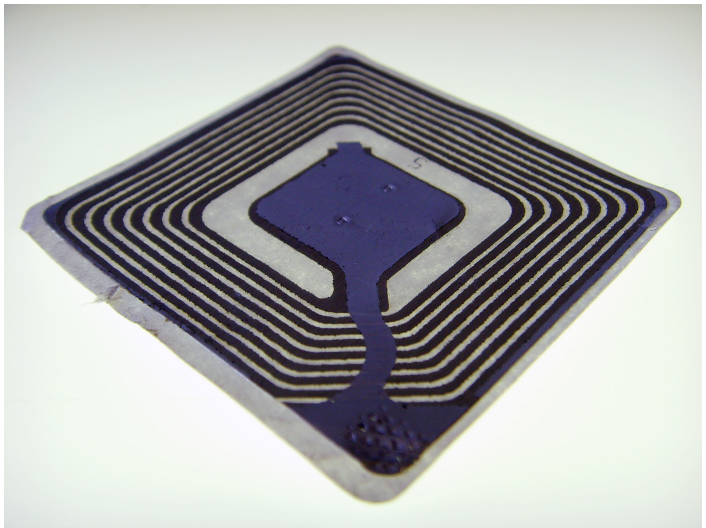
Standard de chiffrement par blocs : AES



- Chiffrement itéré : 10 tours
- Blocs de 128 bits
- Clef de 128 bits
- S-Box de 8 bits appliquée en parallèle sur 16 mots de 8 bits (SubBytes)
- Simple à implémenter
- Bien compris

Cryptographie à bas coût : motivation

- On a des chiffrements symétriques sécurisés et rapides
- Mais leur implémentation est trop coûteuse pour des environnements dédiés...
- Problématique croissante avec la popularité des objets connectés



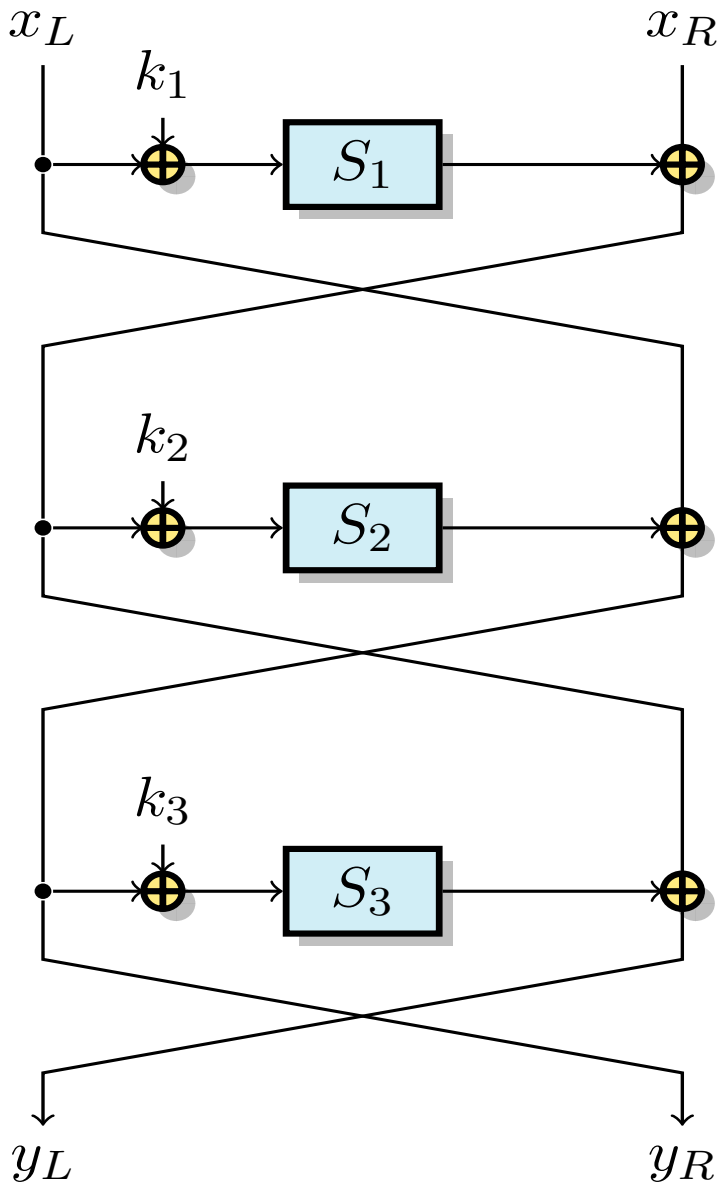
- Taille d'un puce RFID $< 10\,000$ GE
- Taille de la plus petite implémentation d'AES $\sim 10\,000$ GE

Cryptographie à bas coût

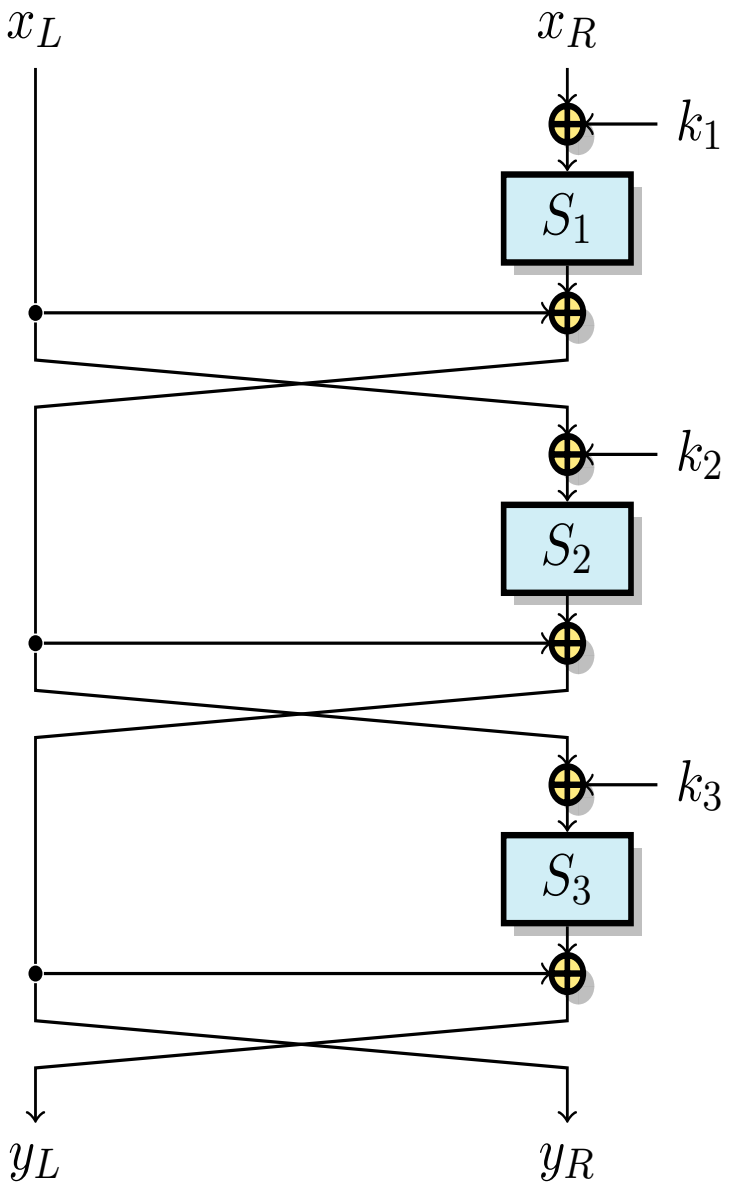
Problématique : les S-Boxes coûtent cher à implémenter

- Taille standard de S-Box : 8 bits (opération sur des octets)
  - L'implémentation reste chère, peut-être trop chère pour le RFID
- De plus petites S-Boxes permettent un coût moins élevé :
  - implémentation logicielle par table : tables plus petites
  - implémentation matérielle : moins de portes logiques
- En revanche, il faut plus de tours pour atteindre la même sécurité
- Peut-on trouver un compromis ?

Construction à partir de S-Boxes plus petites



Feistel



MISTY

Objectif

- Construction de S-Boxes avec des réseaux MISTY et de Feistel
  - En particulier, construction de S-Boxes de 8 bits à partir de S-Boxes de 4 bits
  - Compromis entre coût d'implémentation et paramètres de sécurité

Résultats

- Déterminer les meilleures propriétés atteignables avec les réseaux MISTY et de Feistel
  - Application aux S-Boxes de 8 bits
- En pratique : contruction de S-Boxes à bas coût

Attaques classiques

Attaques différentielles et attaques linéaires

- Attaques statistiques
- Attaques sur le dernier tour
- Distinguer le chiffrement (moins le dernier tour) d'une permutation aléatoire

Pour y résister : la permutation doit avoir les propriétés d'une permutation aléatoire

Le cas des attaques différentielles

- Trouver une différence en entrée de la fonction dx et prédire une différence en sortie dy
- Si il existe une telle différentielle $dx \to dy$ avec probabilité élevée (i.e. beaucoup de solutions à l'équation $F(x) \oplus F(x \oplus dx) = dy$), on pourra distinguer d'une fonction aléatoire

Attaques différentielles

Définition : Uniformité différentielle

Soit F une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2^n$. La table différentielle de F est :

$$\delta_F(a \to b) = \#\{x \in \mathbb{F}_2^n | F(x \oplus a) = F(x) \oplus b\}.$$

De plus, l'uniformité différentielle de F est

$$\delta(F) = \max_{a \neq 0, b} \delta_F(a \to b).$$

On s'intéressera aussi à : $\delta_{\min}(F) = \min_{a \neq 0} \max_b \delta_F(a \to b)$.

- $\delta_F(a \to b)$ est pair
- $\delta(F) = 2$ pour les fonctions APN
- Une S-Box S est résistante aux attaques différentielles si $\delta(S)$ est petite

Table différentielle

dx\dy	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	0	0	0	0	2	2	0	4	0	4	2	0	0
2	0	0	2	4	2	0	0	0	2	4	0	0	0	0	2	0
3	0	2	2	0	4	0	0	0	2	0	0	2	0	0	4	0
4	0	2	0	0	0	0	0	2	0	4	0	2	4	2	0	0
5	0	4	0	0	2	0	0	2	0	0	0	4	0	2	2	0
6	0	0	0	4	0	4	0	0	0	4	4	0	0	0	0	0
7	0	0	2	0	0	4	0	2	2	4	0	0	0	2	0	0
8	0	2	2	2	0	2	0	0	2	0	0	0	2	0	2	2
9	0	0	2	2	2	0	2	0	0	0	0	0	0	2	2	4
10	0	4	2	0	0	0	4	2	0	0	2	0	0	0	0	2
11	0	0	0	0	0	2	2	0	0	0	2	2	2	4	2	0
12	0	0	2	2	2	2	0	0	2	0	0	2	2	0	0	2
13	0	0	0	2	2	0	2	2	2	0	0	0	0	0	2	4
14	0	0	0	0	0	0	4	0	2	0	2	4	0	2	0	2
15	0	2	0	0	2	2	2	4	0	0	2	0	2	0	0	0

Les valeurs sont paires :

$$S(x) \oplus S(x \oplus a) = b \iff S((x \oplus a) \oplus a) \oplus S(x \oplus a) = b$$

Attaques linéaires

Définition : Linéarité

Soit F une fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2^n$. La table des biais linéaires de F est :

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x \oplus b \cdot F(x)}.$$

De plus, la linéarité de F est

$$\mathcal{L}(F) = \max_{a,b \neq 0} |\lambda_F(a, b)|.$$

- Une S-Box S est résistante aux attaques linéaires si $\mathcal{L}(S)$ est petite

Réseaux MISTY et de Feistel

- Initialement : pour définir des chiffrements par blocs (avec clé)
- Bien étudiés, beaucoup de résultats de sécurité sont connus :

$$\mathrm{MEDP}(F_K) = \max_{a \neq 0, b} \frac{1}{2^k} \sum_{K \in \mathbb{F}_2^k} \frac{\delta_{F_K}(a \to b)}{2^n}$$

$$\mathrm{MELP}(F_K) = \max_{a,b \neq 0} \frac{1}{2^k} \sum_{K \in \mathbb{F}_2^k} \left(\frac{\lambda_{F_K}(a,b)}{2^n} \right)^2$$

- Pour MISTY et Feistel :

$$\mathrm{MEDP}(S_i) \leq p \Rightarrow \mathrm{MEDP}(F) \leq p^2$$

$$\mathrm{MELP}(S_i) \leq q \Rightarrow \mathrm{MELP}(F) \leq q^2$$

- Attention ! Ce n'est pas applicable dans le cas où la clé est fixée !

Limite de MEDP

Exemple

- Réseau MISTY sur 3 tours
- $S_1 = S_2 = S_3 = [A, 7, 9, 6, 0, 15, B, 3, E, 8, 2, C, D, 4, F]$.
- $\delta(S_i) = 4$, $\mathrm{MEDP}(S_i) = 2^{-2}$
- $\mathrm{MEDP}(F) \leq 2^{-4}$
- Pour toute clé, il existe une différentielle avec probabilité 2^{-3}

- Une borne sur MEDP signifie :
  1. Choisir une différence en entrée et une différence en sortie
  2. Pour une clé aléatoire, la probabilité différentielle est petite
- Pas de borne lorsque la différence est choisie après la clé !
- En particulier, pour construire une S-Box, il n'y a pas de clé, c'est-à-dire qu'on fixe initialement $K = 0$

Feistel : résultats antérieurs

Théorème (Li et Wang, CHES 2014)

Soit F la fonction construite par 3 tours d'un réseau de Feistel avec les fonctions S_1, S_2 et S_3, alors

- $\delta(F) \geq 2\delta(S_2)$
- $\delta(F) \geq 2^{n+1}$ si S_2 n'est pas une permutation
- Pour $n = 4$, $\delta(F) \geq 8$, et si $\delta(F) = 8$, alors $\mathcal{L}(F) \geq 64$
- $\delta(F) = 8$ et $\mathcal{L}(F) = 64$ est atteignable

Feistel : nouveaux résultats

Théorème

- $\delta(\mathrm{F}) \geq \delta(\mathrm{S}_2)\max(\delta_{\min}(\mathrm{S}_1), \delta_{\min}(\mathrm{S}_3))$
- $\delta(\mathrm{F}) \geq 2^{n+1}$ si S_2 n'est pas une permutation
- $\delta(\mathrm{F}) \geq \max_{i\neq 2, j\neq i,2}(\delta(\mathrm{S}_i)\delta_{\min}(\mathrm{S}_j), \delta(\mathrm{S}_i)\delta_{\min}(\mathrm{S}_2^{-1})$ si S_2 est une permutation
  où $\delta_{\min}(\mathrm{S}) = \min_{a\neq 0}\max_b \delta_{\mathrm{S}}(a \to b)$
- Ces bornes font intervenir les 3 S-Boxes

Pour $n = 4$

- $\delta(\mathrm{F}) \geq 8$, borne atteinte
- $\mathcal{L}(\mathrm{F}) \geq 48$, $\mathcal{L}(\mathrm{F}) \geq 64$ si $\delta(\mathrm{F}) < 32$

MISTY : nouveaux résultats

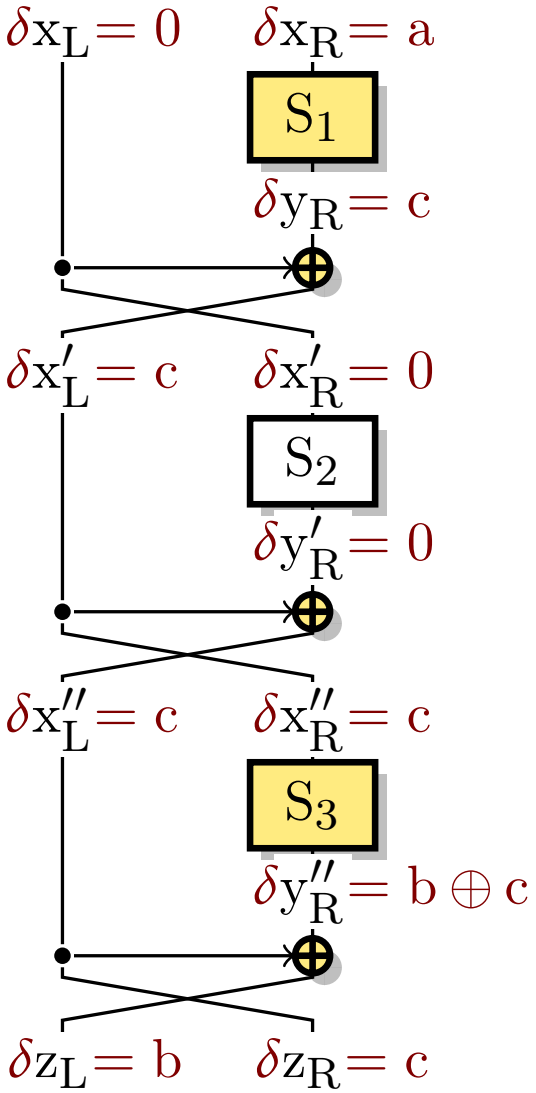
Théorème

- $\delta(F) \geq \delta(S_1) \max(\delta_{min}(S_2), \delta_{min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ si S_1 n'est pas une permutation
- $\delta(F) \geq \max_{i\neq 1, j\neq i,1}(\delta(S_i)\delta_{min}(S_j), \delta(S_i)\delta_{min}(S_1^{-1})$ si S_1 est une permutation
  où $\delta_{min}(S) = \min_{a\neq 0} \max_b \delta_S(a \to b)$
- Il n'y avait aucun résultat précédent sur MISTY à clé fixée

Pour $n = 4$

- $\delta(F) \geq 8$, borne atteinte
- $\mathcal{L}(F) \geq 48$, $\mathcal{L}(F) \geq 64$ si $\delta(F) < 32$

Preuve de sécurité : MISTY



Proposition

$$\delta_F(0 \,\|\, a \to b \,\|\, c) = \delta_{S_1}(a \to c) \times \delta_{S_3}(c \to b \oplus c)$$

Preuve

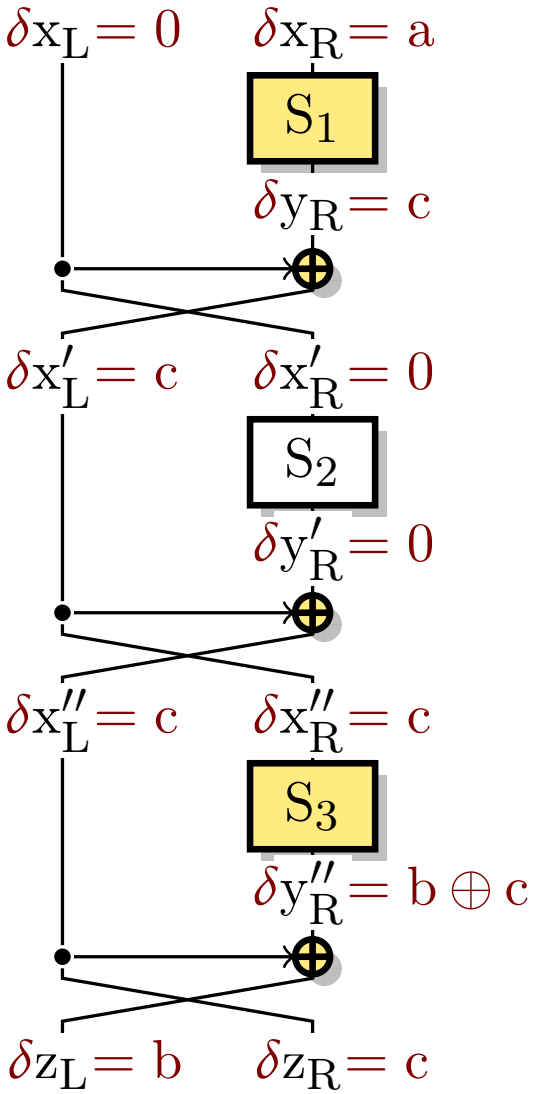
$$F(x_L \| x_R) \oplus F(x_L \| (x_R \oplus a)) = b \| c$$

$$\Leftrightarrow \begin{cases} S_3(S_1(x_R) \oplus x_L) \oplus S_3(S_1(x_R \oplus a) \oplus x_L) = b \oplus c, \\ S_2(x_L) \oplus S_1(x_R) \oplus x_L \oplus S_2(x_L) \oplus S_1(x_R \oplus a) \oplus x_L = c \end{cases}$$

$$\Leftrightarrow \begin{cases} S_3(S_1(x_R) \oplus x_L) \oplus S_3(S_1(x_R \oplus a) \oplus x_L) = b \oplus c, \\ S_1(x_R) \oplus S_1(x_R \oplus a) = c \end{cases}$$

$$\Leftrightarrow \begin{cases} x_R \in D_{S_1}(a \to c) \\ x_L \in S_1(x_R) \oplus D_{S_3}(c \to b \oplus c) \end{cases}$$

Preuve de sécurité : MISTY



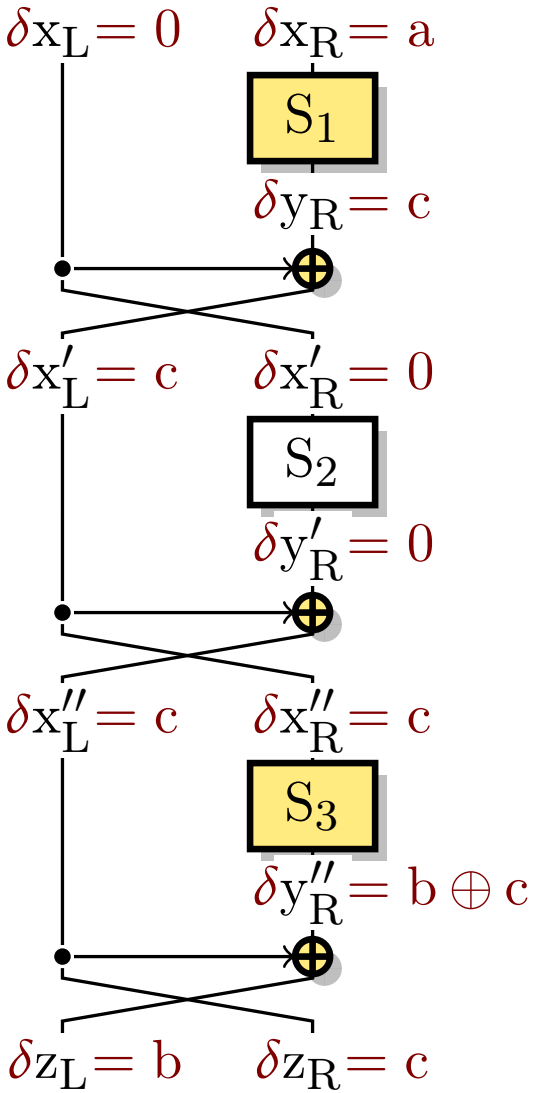
Proposition

$$\delta_F(0 \,\|\, a \to b \,\|\, c) = \delta_{S_1}(a \to c) \times \delta_{S_3}(c \to b \oplus c)$$

Application : si S_1 est non-bijective

- Fixer $b = c = 0$, $\delta_{S_3}(0 \to 0) = 2^n$
- Choisir a tel que $\delta_{S_1}(a \to 0) \geq 2$
- $\delta(F) \geq \delta_F(0 \,\|\, a \to 0 \,\|\, 0) \geq 2^{n+1}$

Preuve de sécurité : MISTY



Proposition

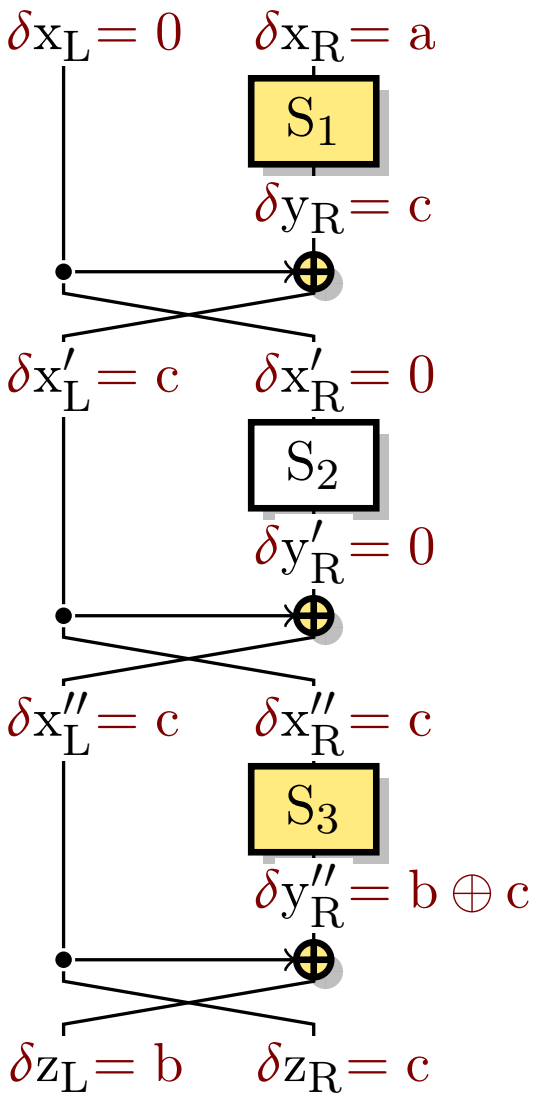
$$\delta_F(0 \,\|\, a \to b \,\|\, c) = \delta_{S_1}(a \to c) \times \delta_{S_3}(c \to b \oplus c)$$

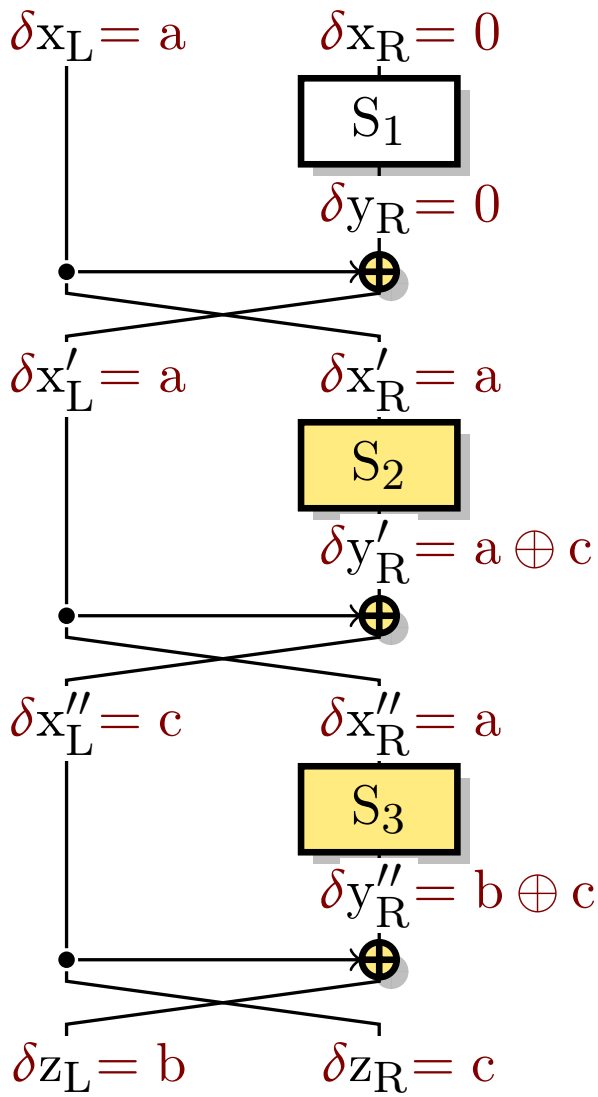
Application : si S_1 est bijective

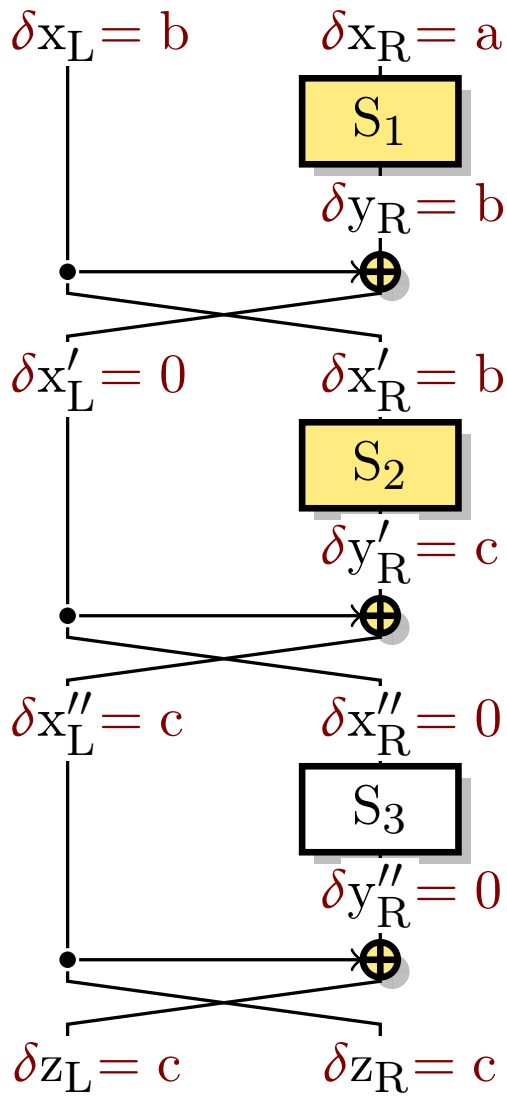
- Choisir a, c tels que $\delta_{S_1}(a, c) = \delta(S_1)$
- Choisir b avec $\delta_{S_3}(c, b \oplus c) \geq \delta_{\min}(S_3)$
- $\delta(F) \geq \delta_F(0 \,\|\, a, b \,\|\, c) \geq \delta(S_1) \times \delta_{\min}(S_3)$

- Choisir b, c tels que $\delta_{S_3}(c, b \oplus c) = \delta(S_3)$
- Choisir a avec $\delta_{S_1}(a, c) \geq \delta_{\min}(S_1^{-1})$
- $\delta(F) \geq \delta_F(0 \,\|\, a, b \,\|\, c) \geq \delta(S_3) \times \delta_{\min}(S_1^{-1})$

Preuve de sécurité : MISTY







Application pour n = 4

Propriétés des S-Boxes de 4 bits

- Classification complète des permutations de 4 bits
  - 302 classes d'équivalence affine [De Cannière ; Leander & Poschmann '07]
- Classification complète des fonctions de 4 bits APN
  - 2 classes d'équivalence affine étendue [Brinkmann & Leander '08]
- Il existe des fonctions de 4 bits APN
  - $\delta(S_i) = 2$, $\delta_{min}(S_i) = 2$
- Il n'existe pas de permutations de 4 bits APN
  - Si S_i est une permutation, $\delta(S_i) \geq 4$, $\delta_{min}(S_i) \geq 2$

Bornes raffinées pour n = 4 (MISTY et Feistel)

- Si S_i toutes non-bijectives, alors $\delta(F) \geq 32$
- Si S_i bijective, $\delta(F) \geq \delta_{min}(S_j) \times \delta(S_i) \geq 8$

MISTY : S-Box de 8 bits avec $\delta(F) = 8$, $\mathcal{L}(F) = 64$

Conditions nécessaires pour $\delta(F) = 8$

- S_1 permutation avec $\delta(S_1) = 4$
- S_2, S_3 APN

Démonstration.

- Supposons $\delta(S_3) \geq 4$
  - $\delta(S_3) \geq 4$, donc il existe c_1, b_1 avec $\delta_{S_3}(c_1 \to b_1) \geq 4$
  - Il y a deux paires $(x, x \oplus c_1)$, $(y, y \oplus c_1)$ dans $D_{S_3}(c_1 \to b_1)$
  - Avec $c_2 = x \oplus y$, $b_2 = S_3(x) \oplus S_3(y)$, il y a deux paires (x, y), $(x \oplus c_1, y \oplus c_1)$ dans $D_{S_3}(c_2 \to b_2)$
  - De même il y a deux paires $(x, y \oplus c_1)$, $(x \oplus c_1, y)$ dans $D_{S_3}(c_1 \oplus c_2 \to b_1 \oplus b_2)$
  - Au moins 3 lignes c_i dans S_3 avec une valeur ≥ 4

MISTY : S-Box de 8 bits avec $\delta(\mathrm{F}) = 8$, $\mathcal{L}(\mathrm{F}) = 64$

Conditions nécessaires pour $\delta(\mathrm{F}) = 8$

- S_1 permutation avec $\delta(\mathrm{S}_1) = 4$
- S_2, S_3 APN

Démonstration.

- Supposons $\delta(\mathrm{S}_3) \geq 4$
  - Au moins 3 lignes $\mathrm{c_i}$ dans S_3 avec une valeur ≥ 4
  - $\delta_{\mathrm{F}}(0||\mathrm{a} \to \mathrm{b}||\mathrm{c}) = \delta_{\mathrm{S}_1}(\mathrm{a} \to \mathrm{c}) \times \delta_{\mathrm{S}_3}(\mathrm{c} \to \mathrm{b} \oplus \mathrm{c})$
  - Pour avoir $\mathrm{c} \leftarrow \mathrm{c_i}$, il faut en plus :
    $\mathrm{c_i}$ colonne de la table des différences de S_1 avec une valeur $= 4$
  - Si un tel $\mathrm{c_i}$ n'existe pas $\Rightarrow \mathrm{L} = \{\mathrm{c}_1, \mathrm{c}_2, \mathrm{c}_3 = \mathrm{c}_1 \oplus \mathrm{c}_2\} \subseteq \mathrm{C}$,
    C = colonnes de S_1 sans valeur $= 4$
  - C pour les représentants des classes par équivalence affine ne contient aucun sous-ensemble stable par XOR

□

S-Box de 8 bits par Feistel et MISTY

Feistel

- $\delta(\mathrm{F}) \geq 8$, borne atteinte
  - Il faut S_1, S_3 APN, S_2 permutation avec $\delta(\mathrm{S}_2) = 4$
- $\mathcal{L}(\mathrm{F}) \geq 48$
  - $\mathcal{L}(\mathrm{F}) \geq 64$ si $\delta(\mathrm{F}) < 32$

MISTY

- $\delta(\mathrm{F}) \geq 8$, borne atteinte
  - Il faut S_2, S_3 APN, S_1 permutation avec $\delta(\mathrm{S}_2) = 4$
  - F n'est pas une permutation
- $\mathcal{L}(\mathrm{F}) \geq 48$
  - $\mathcal{L}(\mathrm{F}) \geq 64$ si $\delta(\mathrm{F}) < 32$
- F permutation : $\delta(\mathrm{F}) \geq 16$, borne atteinte

Construction d'une S-Box résistante à bas coût

- D'après les résultats précédents, le réseau de Feistel est plus adapté
- Il faut S_1, S_3 APN, S_2 permutation avec $\delta(S_2) = 4$
  - Peut-on choisir S_i avec un faible coût d'implémentation ?
- Recherche exhaustive sur les petites implémentations jusqu'à obtenir les bonnes propriétés (Üllrich & al. 2011)
  - Chercher des séquences d'instructions pour une implémentation bit-sliced
  - On utilise des classes d'équivalence pour couper des branches
  - On minimise en particulier les opérations non-linéaires

Exemple concret

Permutation avec $\delta = 4$

- Recherche facile

  On réutilise les résultats de Üllrich & al.
- 9 instructions
  - 4 non-linéaires
  - 4 XOR
  - 1 copie

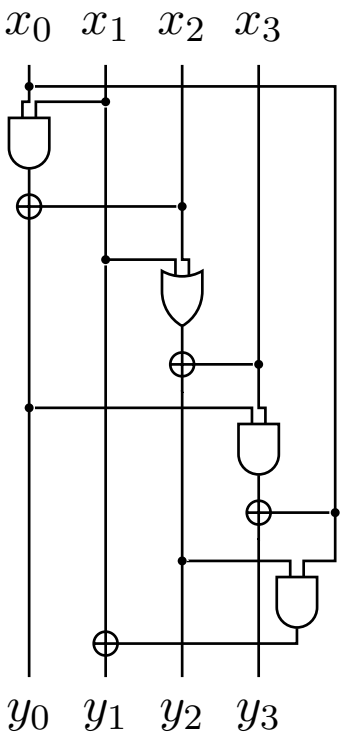
- 4 portes non-linéaires est optimal

Fonction APN

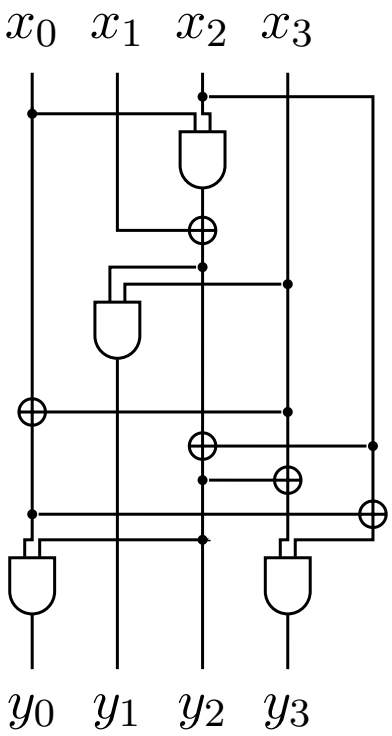
- Recherche coûteuse
  - Pas de filtre pour les permutations
  - 6k core-hours
- 10 instructions
  - Mais 6 non-linéaires
- 11 instructions
  - 4 non-linéaires
  - 5 XOR
  - 2 copies

- 4 portes non-linéaires est optimal

Exemple concret



Permutation avec $\delta = 4$ (S_2)



Fonction APN (S_1, S_3)

Un réseau de Feistel utilisant ces fonctions construit une permutation de 8 bits avec $\delta = 8$ et $\mathcal{L} = 64$.

Résultats

		Implem.		Propriétés		
S-Box	Construction	$\wedge, \vee$	$\oplus$	$\mathcal{L}$	δ	coût
AES	Inversion	32	83	32	4	1
Whirlpool	Lai-Massey	36	58	56	8	1.35
CRYPTON	3-r. Feistel	49	12	64	8	1.83
Robin	3-r. Feistel	12	24	64	16	0.56
Fantomas	3-r. MISTY (3/5 bits)	11	25	64	16	0.51
LS (unnamed)	Whirlpool-like	16	41	64	10	0.64
Nouveau	3-r. Feistel	12	26	64	8	0.45

Conclusion

1. Bornes sur la sécurité des réseaux de Feistel et MISTY à clé fixée
2. Application aux S-Boxes de 8 bits
   - Conditions nécessaires
   - Bornes détaillées pour les permutations
   - Feistel est meilleur pour les S-Boxes inversibles de 8 bits
3. Construction concrète de S-Boxes à bas coût
   - S-Box de 8 bits avec 3 tours de Feistel
   - Amélioration par rapport aux S-Boxes utilisées précédemment

Des questions ?