

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

A. Canteaut, S. Duval, G. Leurent

Inria

05/10/2015

# Table des Matières

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

# Le contexte : les chiffrements par blocs

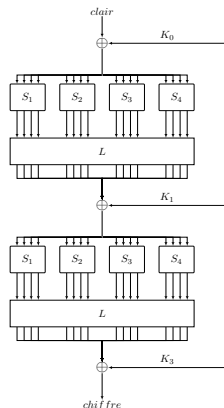
## Critères de Shannon

### 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**



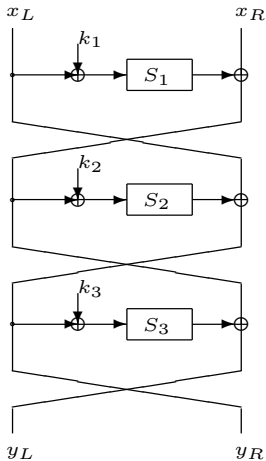
Chiffrement SPN

# Cryptographie à bas coût

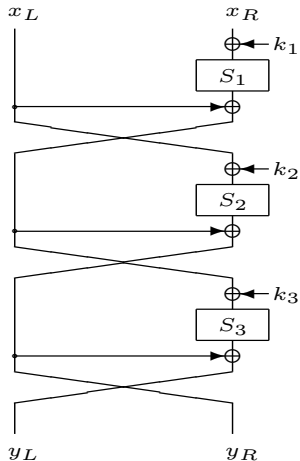
**Problématique** : les S-Boxes coûtent cher à implémenter

- 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 différentielles

### Définition : Uniformité différentielle

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

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

De plus, l'uniformité différentielle de  $F$  est

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

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

## 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 :

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

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

- Pour MISTY et Feistel :

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

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

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

## Limite de MEDP

### Exemple

- Réseau MISTY sur 3 tours
  - $S_1 = S_2 = S_3 = [A, 7, 9, 6, 0, 15, B, 3, E, 8, 2, C, D, 4, F]$ .
  - $\delta(S_i) = 4$ ,  $\text{MEDP}(S_i) = 2^{-2}$
  - $\text{MEDP}(F) \leq 2^{-4}$
  - 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

- $\delta(F) \geq \delta(S_2) \max(\delta_{\min}(S_1), \delta_{\min}(S_3))$
- $\delta(F) \geq 2^{n+1}$  si  $S_2$  n'est pas une permutation
- $\delta(F) \geq \max_{i \neq 2, j \neq i, 2}(\delta(S_i) \delta_{\min}(S_j), \delta(S_i) \delta_{\min}(S_2^{-1}))$  si  $S_2$  est une permutation  
où  $\delta_{\min}(S) = \min_{a \neq 0} \max_b \delta_S(a \rightarrow b)$
- Ces bornes font intervenir les 3 S-Boxes

Pour  $n = 4$

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

## 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  $\delta_{\min}(S) = \min_{a \neq 0} \max_b \delta_S(a \rightarrow b)$
- **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  $\delta(F) < 32$

## S-Box de 8 bits par Feistel et MISTY

### Feistel

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

### MISTY

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

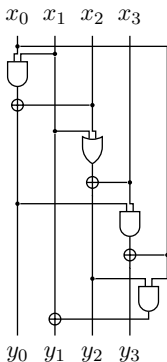
### Fonction APN

- **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

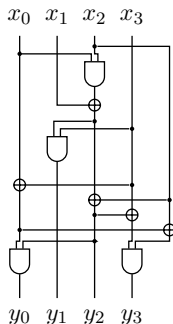
- 4 portes non-linéaires est **optimal**



# 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

S-Box	Construction	Implem.		Propriétés		
		$\wedge, \vee \oplus$	$\mathcal{L}$	$\delta$	coût	
AES	Inversion	32	83	32	4	1
Whirlpool	Lai-Massey	36	58	64	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
<b>Nouveau</b>	<b>3-r. Feistel</b>	<b>12</b>	<b>26</b>	<b>64</b>	<b>8</b>	<b>0.45</b>

# 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 ?