Les réseaux de Feistel classiques et généralisés

Franck Jeannot

Montréal, Canada, Février 2018, Q485, v1.0

Abstract

A review of Feistel networks with some classical and generalized examples.

Keywords: Feistel Networks, XOR, bloc cipher, block-cipher cryptanalysis, chiffrements par blocs, rondes, S-Boxes, GFS, RC6, round function

1. Introduction

Un *réseau de Feistel*[1] [2] est une construction utilisée dans les algorithmes de ***chiffrements par blocs***, conçu par le cryptologue d'IBM, Horst **Feistel** [1] [2] . Il est fait diverses **transformations** sur des blocs dans le but de chiffrer le texte initial. Si les actions sont répétitives, on parlera de **ronde**. La fonction ($\oplus$) **XOR** est souvent utilisée, par exemple en « *blanchiement de clé* » ou ***key withening***[3]. Exemple de **ronde d'expansion de Feistel**[4] :

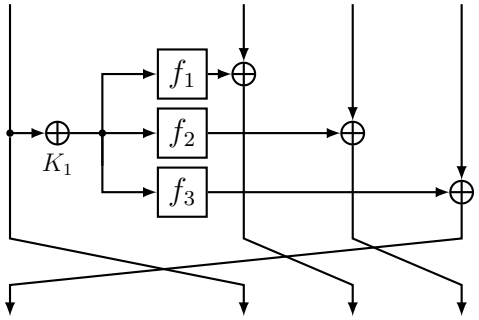

FIGURE *(1): Expanding Feistel round function. Référence : www.iacr.org*

1. https://eprint.iacr.org/2010/301.pdf
2. https://en.wikipedia.org/wiki/Feistel_cipher
3. https://en.wikipedia.org/wiki/Key_whitening
4. http://www.cs.utsa.edu/~wagner/laws/AESkeys.html

Il existe de multiples types de résaux de Feistel dits ***classiques*** et ***généralisés***. « *Un réseau de Feistel repose sur des principes simples dont des permutations, des substitutions, des échanges de blocs de données et une fonction prenant en entrée une clé intermédiaire à chaque étage.* » [5]

2. Chiffrement par flot et chiffrement par bloc

2.1. Chiffrement par flot

Un chiffrement par flot (*ou chiffrement de flux*) se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un **XOR** entre un bit à la sortie du générateur et un bit provenant des données. Toutefois, le XOR n'est pas la seule opération possible ; la seule contrainte sur cette opération est qu'elle doit être inversible (la disjonction exclusive est même involutive), comme l'opération d'addition dans un groupe est également envisageable . [6]

2.2. Chiffrement par bloc

Le chiffrement par bloc (en anglais ***block cipher***) utilise un découpage des données en blocs de taille généralement fixe.

3. Algorithme ou fonction XOR

La fonction *OU exclusif*, dite **XOR** (*de* ***X****clusive* ***OR***)) [7], est un opérateur logique de l'**algèbre de Boole**. Son symbole en cryptographie est un "*plus dans un cercle*" (`oplus`) $\oplus$ ou bien (`"veebar"`) $\veebar$ en *algèbre relationnelle*. Sa défintion peut se simplifier en "Le résultat R est VRAI si un et un seul des opérandes A et B est VRAI" [8], soit $R = A \oplus B$.
On trouve de nombreuses autres représentations de la fonction XOR. [9]

5. https://fr.wikipedia.org/wiki/R%C3%A9seau_de_Feistel
6. https://fr.wikipedia.org/wiki/Chiffrement_par_flot
7. https://morf.lv/introduction-to-data-encryption
8. https://fr.wikipedia.org/wiki/Fonction_OU_exclusif
9. https://en.wikipedia.org/wiki/Exclusive_or

4. Cryptanalyse de chiffrement par bloc

Voir *A self-study course in Block cipher Analysis* de Bruce Schneier [10]
FEAL est un *cipher* classique en cryptanalyse [3].

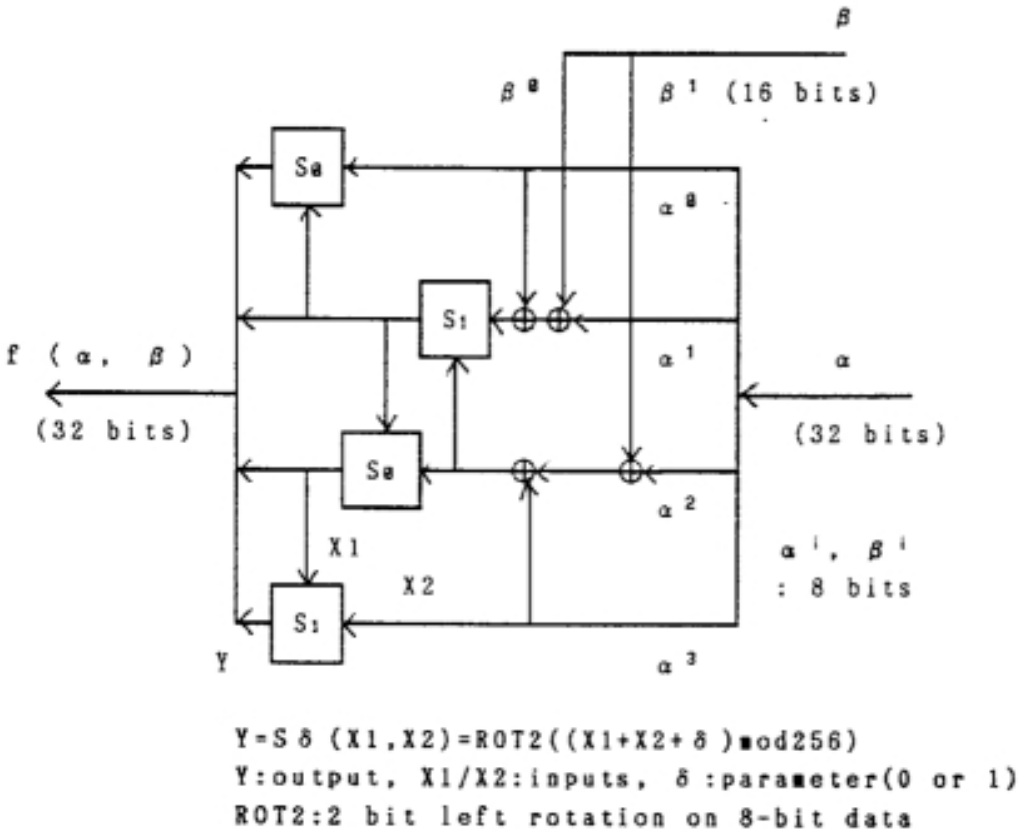

FIGURE *(2): le détail de la fonction f de FEAL et ses sous-fonctions. Source Shimizu-Miyaguchi-1998 fig 3 p. 274*

Ici $S(X1, X2, \delta) = ROT2\ (T)$ avec $T = X1 = X2 + \delta\ mod\ 256$ et X1, X2 et T sont des blocs de 1 octet
$\delta = 0$ *ou* 1 (valeur constante) et $ROT2\ (T)$ est le résultat d'une "*2 bit left rotation*" sur T.

10. https://www.schneier.com/academic/paperfiles/paper-self-study.pdf

5. S-boxes

Une S-Box [11] [12] (*substitution box*), est une table de **substitution** utilisée dans un algorithme de chiffrement symétrique. Une S-Box correctement conçue pour de la cryptographie va respecter les **notions de confusion et diffusion** introduites en 1945 par Claude Shannon [13] [14].

6. Feistel classiques - Types 1 à 3

Parmis les réseaux de Feistel **classiques**, certains ont été classés [4] suivant leurs caractéristiques en Type 1 à Type 3. [15] On nomme **L** le bloc de gauche (**L**eft) et **R** le bloc de droite (**R**ight) et pour chaque ronde une fonction F_i est introduite. Les fonctions **F** sont des *substitutions* basées notamment sur S-boxes. [16] [17]

6.1. Feistel - Type 1 : exemple

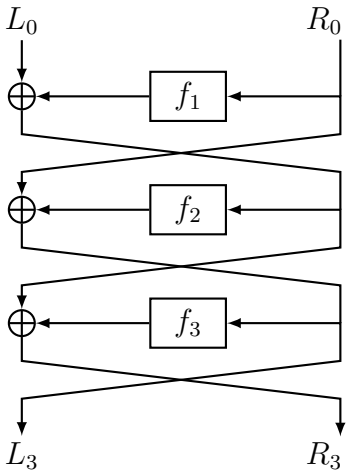

FIGURE *(3): 3-round Feistel-1. Référence : www.iacr.org*

11. https://fr.wikipedia.org/wiki/S-Box
12. https://en.wikipedia.org/wiki/Rijndael_S-box
13. https://en.wikipedia.org/wiki/Confusion_and_diffusion
14. https://www.iacr.org/museum/shannon45.html
15. https://pdfs.semanticscholar.org/60ab/c36e684e3c8e6b689bb19cbc74e56b00d92c.pdf
16. https://tools.ietf.org/html/rfc4086
17. http://www.ciphersbyritter.com/RES/SBOXDESN.HTM

6.2. Feistel - Type 2 : exemple

L'exemple suivant est la symbolisation d'un réseau de Feistel de *type 2* avec deux **rondes** ou *deux tours* (**2-round Feistel-2**). Une clé K_i est introduite à chaque ronde :

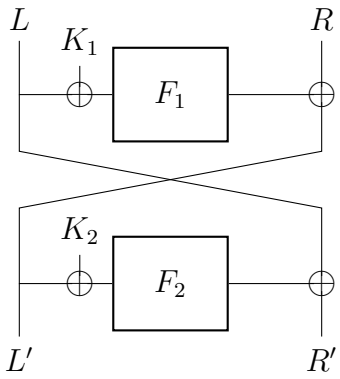

FIGURE *(4): 2-round Feistel-2. Référence : www.iacr.org*

7. Generalized Feistel Structure et types généralisés

Voir GFS [18] et "*Generalized Feistel Networks*" [19]
RC6 [20] [21] est un Type 2 généralisé.

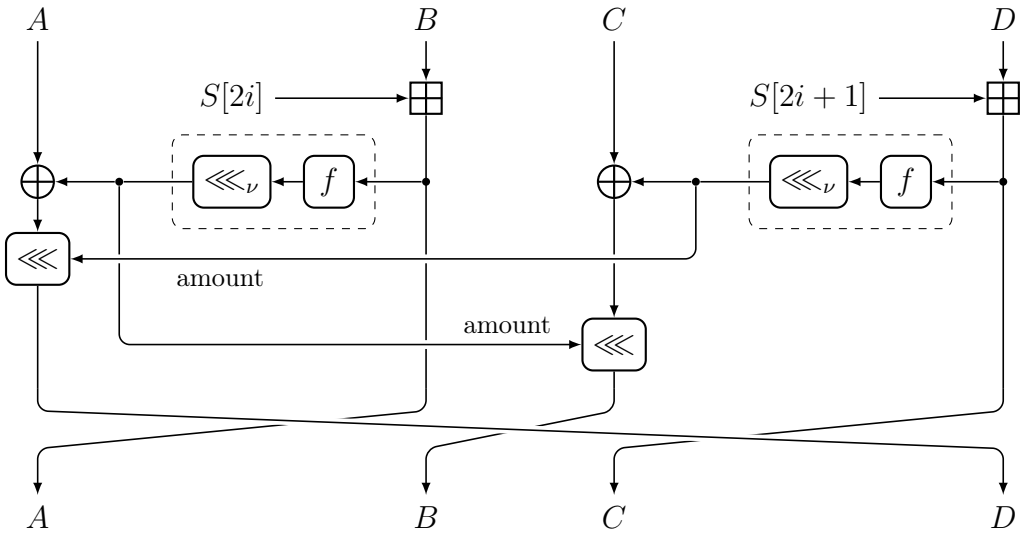

FIGURE *(5): RC6 Round Function. Référence : www.iacr.org*

MARS [22] est un Type-3 généralisé.

18. https://www.iacr.org/archive/fse2010/61470020/61470020.pdf
19. http://cryptowiki.net/index.php?title=Generalized_Feistel_networks
20. https://en.wikipedia.org/wiki/RC6
21. https://www.google.com/patents/US5724428
22. https://en.wikipedia.org/wiki/MARS_(cryptography)

Références

[1] H. Feistel, W. A. Notz, J. L. Smith, Some cryptographic techniques for machine-to-machine data communications, Proceedings of the IEEE 63 (11) (1975) 1545–1554. doi:10.1109/PROC.1975.10005.

[2] H. Feistel, Cryptography and Computer Privacy, Scientific American 228 (1973) 15–23. doi:10.1038/scientificamerican0573-15.

[3] A. Shimizu, S. Miyaguchi, Fast data encipherment algorithm feal, in : D. Chaum, W. L. Price (Eds.), Advances in Cryptology — EUROCRYPT' 87, Springer Berlin Heidelberg, Berlin, Heidelberg, 1988, pp. 267–278.

[4] Y. Zheng, T. Matsumoto, H. Imai, On the construction of block ciphers provably secure and not relying on any unproved hypotheses, in : G. Brassard (Ed.), Advances in Cryptology — CRYPTO' 89 Proceedings, Springer New York, New York, NY, 1990, pp. 461–480.