Diffusion totale dans le schéma de Feistel généralisé

S. Delaune, P. Derbez, **A. Gontier**, C. Prud'homme

ANR DECRYPT: analyse de la crypto symétrique avec la CP

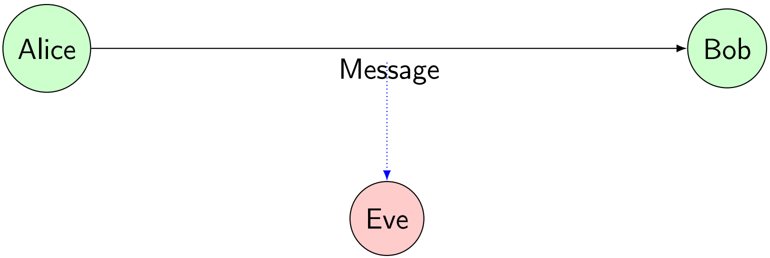
23 février 2022

Sommaire sommaire

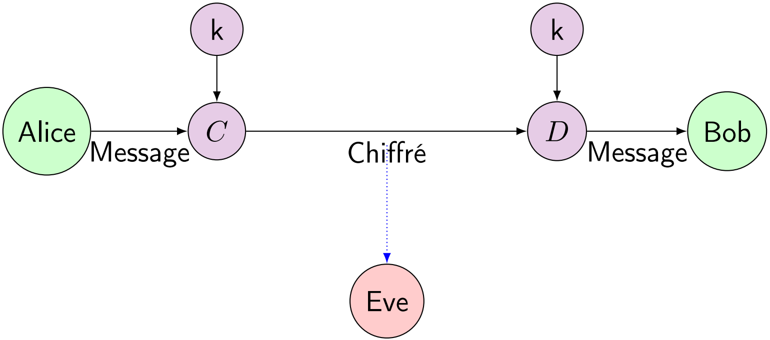
1. Le schéma de chiffrement de feistel
   - Permutation
   - Diffusion
   - Even-odd et borne de Fibonacci

2. Étude du cas non even-odd
   - Modèles CP
   - Construction des chemins

La crypto symétrique



La crypto symétrique



k : clef privée partagée

C : fonction de chiffrement

D : fonction de déchiffrement

Sommaire de section

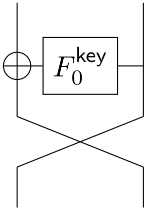
Feistel : un chiffrement symétrique par bloc

Une clef secrète partagée qui chiffre et déchiffre :

Chiffré = Chiffrement(Message,k)

Message = Déchiffrement(Chiffré,k)

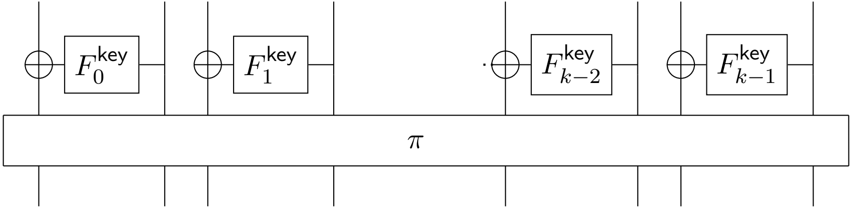
Un découpage du message en blocs, les paires de Feistel :



Feistel généralisés

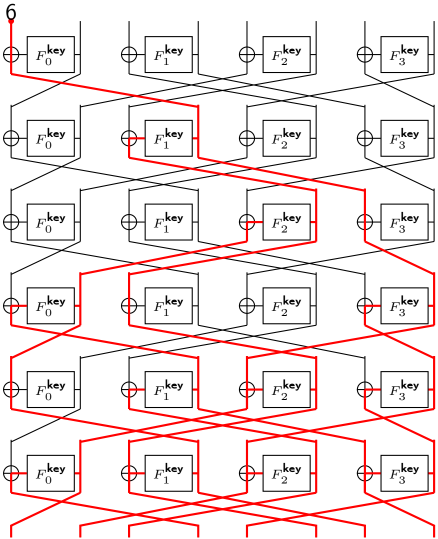
Un tour du schéma de Feistel généralisé [1] :

- Un xor par paire
- Une permutation π



Rapide ET Résistant ? : la diffusion max[1]

Exemple de diffusion



Definition (Diffusion)

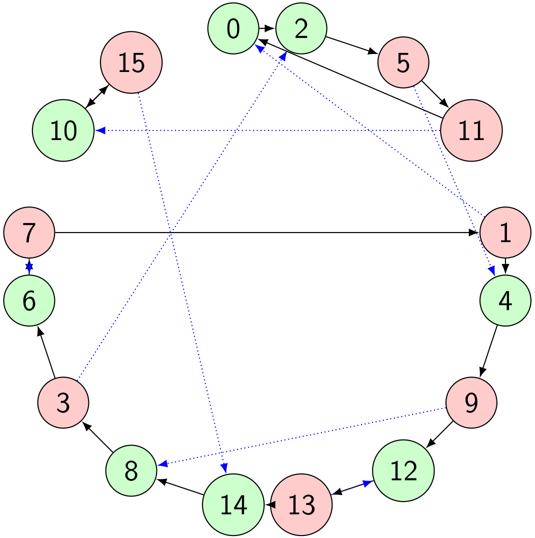
Nombre de tour pour qu'un bloc soit mélangé dans tous les bloc

Definition (Diffusion max[1])

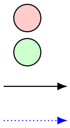
Maximum de la diffusion de chaque bloc

On cherche π qui minimise la diffusion max

Représentation en graphe de la permutation de Feistel



Légende :



Epsilon transition :

Mélange des blocs impairs dans les pairs avant la permutation

Diffusion en τ tours

Pour toute paire de noeud (i, j), il existe au moins un chemin de taille exactement τ qui vas de i vers j.

Représentation en graph

Remarque

Tous les nœuds atteignent tous les nœuds en τ *transitions si et seulement si tous les nœuds verts atteignent tous les nœuds rouges en* $\tau - 1$ *transitions [2]*

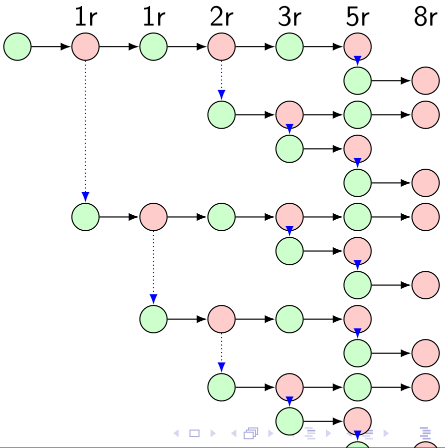
Démonstration.

Les nœuds verts de départ sont epsilon-reliés aux rouges.
Les nœuds rouges d'arrivée sont epsilon-reliés aux verts donc au tour suivant tous les nœuds sont atteints. $\square$

Le cas even-odd

Definition

Une permutation even-odd envoie tous les blocs pairs sur des impairs et inversement



Des méthodes spécifiques efficaces pour le cas even-odd [2].

Une borne théorique : la borne de Fibonacci

Des graphs plus équilibrés et moins nombreux

Le cas non even-odd diffuse-t-il mieux ?

Sommaire de section

Les Variables CP

Variables

- Variables booléennes : la matrice d'adjacence du graphe
- Variables entières : unique successeur de chaque noeud
- Variables ensemblistes : ensemble des successeurs de chaque noeud
- Variable graphe

Contraintes de Feistel

- Contrainte sur les arcs doublants
- Sommes sur la matrice
- Alldifferent

Comment contraindre la diffusion ?

Produit matriciel

On modélise la permutation de feistel dans le graphe et on déclare ce graphe par sa matrice d'adjacence. $A = \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{matrix}$

À cette matrice on doit ajouter les arcs doublants : $B = A + D = \begin{matrix} 0 & 1 & 0 & 0 \\ 0 & \color{red}{1} & 0 & 1 \\ 1 & 0 & 0 & 0 \\ \color{red}{1} & 0 & 1 & 0 \end{matrix}$

On peut ensuite calculer la matrice à la puissance τ pour savoir si il y a bien tous les chemins

$$B^4 = \begin{matrix} 2 & 2 & 1 & 1 \\ 2 & 4 & 1 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{matrix}$$

Produit matriciel

Relaxation des produits matriciels dans les booléen

Exponentiations rapides

Modèles minizinc testés avec plusieurs solveurs (Chuffed $<$ OrTools $<$ Picat $<$ Gurobi)
Remarque : Le CDCL (LCG) ne fait pas une grande différence

Un modèle plus proche de la CP ?

Diffusion avec des unions

Soit S_{i1}, l'ensemble des successeurs du nœud i et $S_{i,\tau}$, l'ensemble des nœuds atteignables au tour $\tau > 1$ depuis le nœud i.

$$\begin{array}{c||c|c|c}
S_{0,1} & S_{0,2} & S_{0,3} & S_{0,4} \\
S_{1,1} & S_{1,2} & S_{1,3} & S_{1,4} \\
S_{2,1} & S_{2,2} & S_{2,3} & S_{2,4} \\
S_{3,1} & S_{3,2} & S_{3,3} & S_{3,4}
\end{array}$$

La diffusion au tour τ depuis le nœud i s'écrit comme l'union des diffusions atteintes par i au tour précèdent :

$$S_{i,\tau} = \bigcup_{j \in S_{i,\tau-1}} S_{j,1}$$

Diffusion avec des unions

Nous avons ajouté la contrainte union avec l'indice comme variable ensembliste au solveur Choco.

On peut atteindre 24 blocs en moins d'une heure (précédentes méthodes à 18 blocs)

Objectif : comparaison avec le cas even-odd pour 32 blocs.

Comment réduire l'espace de recherche ?

Symétries

On peut casser des symétries sur une permutation. (contrainte, stratégie ou déclaration des domaines)

Mais les symétries de Feistel marchent par **paires de blocs**.

Proposition : On contraint dynamiquement les domaines des variables pour n'avoir toujours qu'une seule paire libre disponible pendant la résolution.

$\Longrightarrow$ Ne contraint pas assez pour se comparer a l'even-odd , comment faire mieux ?

Construction des chemins

Intuition : la taille des chemins augmente moins vite que le nombre de paires de feistel.

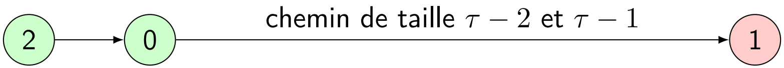
On crée tous les chemins de chaque nœud vers tous les autres tant qu'il reste des nœuds et des rounds τ.

$$0 \xrightarrow{\text{chemin de taille } \tau - 1} 1$$

Construction des chemins

Intuition : la taille des chemins augmente moins vite que le nombre de paires de feistel.

On crée tous les chemins de chaque nœud vers tous les autres tant qu'il reste des nœuds et des rounds τ.



Construction des chemins

Intuition : la taille des chemins augmente moins vite que le nombre de paires de feistel.

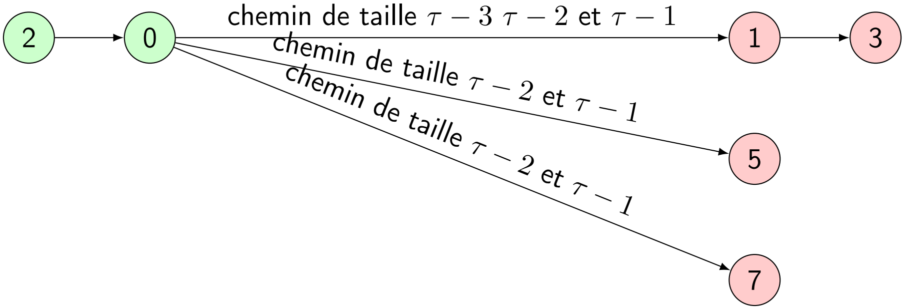
On crée tous les chemins de chaque nœud vers tous les autres tant qu'il reste des nœuds et des rounds τ.

$$2 \longrightarrow 0 \xrightarrow{\text{chemin de taille } \tau - 3 \ \tau - 2 \text{ et } \tau - 1} 1 \longrightarrow 3$$

Construction des chemins

Intuition : la taille des chemins augmente moins vite que le nombre de paires de feistel.

On crée tous les chemins de chaque nœud vers tous les autres tant qu'il reste des nœuds et des rounds τ.



Construction des chemins

La numérotation progressive des noeuds casse des symétries (mais il en reste)

Même ordre de complexité que les modèles CP en pratique.

Une stratégie CP ?

Conclusion

Le cas non even-odd de la diffusion de Feistel est intuitivement déséquilibré mais peut-il avoir **une meilleur diffusion totale ?**

- La complexité du cas non even-odd est grande avec beaucoup de symétries sur les paires de Feistel
- La construction de chemins permet de casser des symétries mais est difficilement compatible avec les modèles CP

Nos modèles sont efficaces par rapport aux anciens travaux sur les permutations non even-odd mais doivent être améliorés pour confirmer ou infirmer l'intuition du cas even-odd

Bibliographie

[1] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized feistel. In Seokhie Hong and Tetsu Iwata, editors, Fast Software Encryption, 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010, Revised Selected Papers, volume 6147 of Lecture Notes in Computer Science, pages 19–39. Springer, 2010.

[2] Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Victor Mollimard. Efficient search for optimal diffusion layers of generalized feistel networks. IACR Transactions on Symmetric Cryptology, 2019(2) :218–240, Jun. 2019.

Filtrage de l'Union

On peut trouver les règles de filtrage suivantes :

$$u \notin \overline{S_i},\ i \in \overline{I},\ \forall j \in \overline{I}, j \neq i,\ u \notin \overline{S_j} \implies u \notin \overline{U}$$

$$u \in \underline{S_i},\ i \in \underline{I} \implies u \in \underline{U}$$

$$i \notin \overline{I},\ \forall u \in \overline{S_i},\ \forall j \in \overline{I}, j \neq i,\ u \notin \overline{S_j} \implies u \notin \overline{U}$$

$$i \in \underline{I},\ u \in \underline{S_i} \implies u \in \underline{U}$$

$$u \notin \overline{U},\ \exists i \in \overline{I},\ \forall j \in \overline{I}, j \neq i,\ u \notin \overline{S_j} \implies u \notin \overline{S_i}$$

$$u \in \underline{U},\ \exists i \in \underline{I},\ \forall j \in \underline{I}, j \neq i,\ u \notin \overline{S_j} \implies u \in \underline{S_i}$$