TD5 - Cryptanalyse Différentielle

Responsable : M. Bombar

1 Cryptanalyse Différentielle de FEAL - Examen 2021

1.1 Notations

Dans cet exercice, si $x \in \mathbb{F}_2^n$ et $y \in \mathbb{F}_2^m$ sont deux chaînes de bits, représentés par des vecteurs binaires, alors $x \,||\, y \in \mathbb{F}_2^{n+m}$ est le vecteur binaire représentant leur **concaténation**.

Par ailleurs, les boîtes S de FEAL agissant sur des octets parfois vus comme des éléments de $\mathbb{Z}/256\mathbb{Z}$, ou bien comme des vecteurs de 8 bits dans $\mathbb{F}_2^8$, on notera $\oplus$ l'addition dans l'espace vectoriel $\mathbb{F}_2^8$ (donc le XOR bit à bit), et $\boxed{+}$ l'addition modulo 256.

Enfin, pour n un entier non nul, on notera $\mathbf{0}_n \in \mathbb{F}_2^n$ pour désigner le vecteur nul de longueur n. Par exemple $\mathbf{0}_3 = 000$.

1.2 Le chiffrement FEAL

FEAL (*Fast Data Encipherment Algorithm*) est un chiffrement par blocs de type Feistel à 4 tours qui utilise des clés de 64 bits pour chiffrer des blocs de 64 bits. Il a été proposé par A. Shimizu et S. Miyaguchi en 1987 dans le but de remplacer le chiffrement DES et ses clés de 56 bits.

Les clés. FEAL utilise 2 clés K_0 et K_5 de 64 bits, et 4 sous clés de 16 bits K_1, K_2, K_3, K_4.

Les boîtes S. FEAL utilise deux boîtes S différentes notées S_0 et S_1 prenant en entrée 16 bits représentés comme une paire d'entiers dans $\{0, \ldots, 255\}$ et produisant 8 bits en sortie. Elles sont définies comme suit :

$$S_i(x, y) = (x \boxed{+} y \boxed{+} i \mod 256) <<< 2.$$

où $<<< 2$ désigne une rotation de 2 bits vers la gauche (de façon cyclique).

La fonction de tour. FEAL utilise 4 tours de type Feistel dont les fonctions de tours, notées F_{K_i} pour $1 \leq i \leq 4$, prennent en entrée 32 bits et ressortent 32 bits. Soit M un bloc de 64 bits à chiffrer. On pose $X_0 \overset{\text{def}}{=} M \oplus K_0 = (L_0 \,||\, R_0)$, où L_0 (resp. R_0) désigne les 32 bits les plus à gauche (resp. les plus à droite) de X_0. On rappelle que dans un schéma de Feistel en notant pour $1 \leq i \leq 4$ $X_i = (L_i \,||\, R_i)$ les 32 bits en sortie du tour i, on a

$$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus F_{K_i}(R_{i-1}).$$

Le chiffré est alors

$$C = (R_4 \,||\, L_4) \oplus K_5.$$

Pour $X = (x_0 \,||\, x_1 \,||\, x_2 \,||\, x_3)$ de 32 bits, vu comme la concaténation de 4 octets, et $K = (K^L \,||\, K^R)$ une clé de 16 bits, la fonction $F_K(X)$ est définie par

$$F_K(X) \stackrel{\text{def}}{=} S_0(x_0, u) \,||\, u \,||\, v \,||\, S_1(x_3, v),$$

avec

$$u = S_1(x_0 \oplus x_1 \oplus K^L, x_2 \oplus x_3 \oplus K^R)$$

et

$$v = S_0(x_2 \oplus x_3 \oplus K^R, u).$$

(Q1) Montrer que pour tout $(x, y) \in \mathbb{F}_2^8 \times \mathbb{F}_2^8$, on a

$$S_0(x \oplus 1000\ 0000, y) = S_0(x, y) \oplus 0000\ 0010.$$

(Q2) Soient $M, M^\star \in \mathbb{F}_2^{64}$ deux messages clairs tels que

$$M \oplus M^\star = 1000\ 0000\ 1000\ 0000\ \mathbf{0}_{48}.$$

On note $(L_2 \,||\, R_2)$ (resp. $(L_2^\star \,||\, R_2^\star)$) l'entrée du troisième tour lors du chiffrement de M (resp. de $M^\star$). Que vaut la différence

$$(L_2 \,||\, R_2) \oplus (L_2^\star \,||\, R_2^\star)?$$

(Q3) Soit $K = K^L \,||\, K^R$ une sous clé de 16 bits, avec K^L et K^R sur 8 bits. Montrer que pour tout X de 32 bits, on a

$$F_K(X) = F_{\mathbf{0}_{16}}(X \oplus (0000\ 0000 \,||\, K^L \,||\, K^R \,||\, 0000\ 0000)).$$

(Q4) On note $K_5 \stackrel{\text{def}}{=} K_5^L \,||\, K_5^R$ avec K_5^L, K_5^R de 32 bits, et de même $K_4 = K_4^L \,||\, K_4^L$ avec K_4^L, K_4^R de 8 bits.
Déduire des deux questions précédentes une attaque utilisant 2 clairs choisis et permettant de retrouver la valeur de $K_5^R \oplus (0000\ 0000 \,||\, K_4^L \,||\, K_4^R \,||\, 0000\ 0000)$ en évaluant un certain nombre de fois N la fonction de tour F. Quelle est la valeur de N ?
Indication : Raisonner autour de $F_{K_4}(L_4) \oplus F_{K_4}(L_4^\star)$.

On peut alors montrer qu'en itérant l'attaque précédente sur tous les tours, on peut retrouver une clé équivalente de FEAL en 2^{35} évaluations de la fonction F, à l'aide de plusieurs propriétés différentielles.

2 Un chiffrement par bloc simple

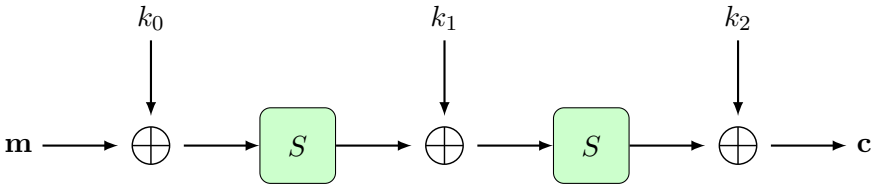

FIGURE 1 – Un chiffrement à deux tours sans permutation

On considère le chiffrement présenté en Figure 1, constitué de deux Sbox de 4 bits dont la table de valeurs est donnée en Figure 2 en écriture hexadécimal [1]. Dans ce système de chiffrement, les couches linéaires sont assurées par les additions de clés, et il n'y a pas de permutation des bits supplémentaire. L'objectif de ce TP est de mettre en place une cryptanalyse différentielle contrre ce systèmee de chiffrement.

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

Les clés k_i possèdent toutes 4 bits pour le moment.

(Q5) Quel est le coût de la recherche exhaustive pour retrouver les clés ?

En particulier, dans cet exemple jouet, on pourrait tout à fait faire une attaque par force brute pour récupérer les clés. L'idée est qu'il est suffisamment simple pour que vous puissiez suivre à la main les étapes de la cryptanalyse différentielle, mais on va voir que celle-ci passe extrêmement bien à l'échelle sur ce type de chiffrement. Une fois l'esprit de cette technique de cryptanalyse bien comprise, ses généralisations en rajoutant plusieurs tours, et autres permutations linéaires devraient se faire sans trop de problème autres que des problèmes techniques d'implémentation, peut-être.

1. J'ai généré cette boîte S comme une fonction booléenne bijective $\mathbb{F}_2^4 \to \mathbb{F}_2^4$. La morale de l'histoire c'est **Don't roll your own crypto !** Décrire des boîtes S qui résistent aux attaques est quelque chose d'extrêmement difficile.

(Q6) Implémentez le chiffrement en Python ou Sage, à votre convenance [a]. Essayez d'être le plus flexible possible quant à la valeur de la boîte S, ou encore du nombre de tours, ça pourra vous être utile par la suite. On pourra générer les clés comme des entiers aléatoires écrits sur 4 bits.

(Q7) Déterminez la table distribution des différences de S.

(Q8) Quelle est l'uniformité différentielle de S ?

(Q9) Déterminez une caractéristique différentielle pertinente pour la cryptanalyse de ce chiffrement. Quelle est sa probabilité d'apparition ?

a. Ou autre si vous préférez !

2.1 Simplification : Chiffrement à un tour unique

Pour commencer, on va supposer que ce chiffrement ne possède qu'un seul tour.

(Q10) Décrivez les étapes de la cryptanalyse différentielle de ce système de chiffrement à un tour unique.

(Q11) Écrivez une fonction, par exemple de la forme `gen_possible_intermediate_value(Sbox, a, b)` qui calcule toutes les paires $((\widetilde{\mathbf{m}}, \widetilde{\mathbf{m}'}), (\widetilde{\mathbf{c}} = S(\widetilde{\mathbf{m}}), \widetilde{\mathbf{c}'} = S(\widetilde{\mathbf{m}'}))$ de couples clairs-chiffrés tels que $\Delta(\mathbf{m}) = \alpha$, $\Delta(\mathbf{c}) = \beta$.

(Q12) Écrivez une fonction `gen_plain_cipher_pair` qui prend en argument un entier α et un entier N, et renvoie N paires de couples clairs-chiffrés $(\mathbf{m}, \mathbf{m}'), (\mathbf{c}, \mathbf{c}')$ tels que $\Delta(\mathbf{m}) \stackrel{\text{def}}{=} \mathbf{m} \oplus \mathbf{m}' = \alpha$ et $\mathbf{c}$ (resp. $\mathbf{c}'$) est le chiffré complet de $\mathbf{m}$ (resp. $\mathbf{m}'$). Cette fonction aura donc accès aux clés secrètes k_0 et k_1, et jouera le rôle d'un oracle de chiffrement.

(Q13) Écrivez une fonction `find_good_pair` qui prend en entrée une différentielle $(\alpha \mapsto \beta)$ et renvoie **une** paire de couples clairs-chiffrés satisfaisant à cette différentielle.

(Q14) Terminez d'implémenter la cryptanalyse différentielle en retrouvant la clé secrète complète. De combien de paires de clairs-chiffrés connus avez-vous besoin ?

(Q15) Testez votre attaque en variant la boîte S, les clés, et surtout la **taille** des blocs. Vérifiez en pratique que votre attaque passe bien à l'échelle (tant que vous êtes en mesure de stocker suffisamment de données).

2.2 Augmenter le nombre de tours

(Q16) Rappelez le principe de la cryptanalyse différentielle d'un système de chiffrement à plusieurs tours.

(Q17) Implémentez la cryptanalyse différentielle de ce système de chiffrement dans le cas de deux tours.

(Q18) Pour tester votre attaque, faites comme précédemment en faisant varier la boîte S, les clés et la taille des blocs.

Remarque : Puisqu'il s'agit d'une attaque **probabiliste**, elle peut échouer, et il faut parfois recommencer en relançant l'attaque pour parvenir à ses fins.

(Q19) Vérifiez de même que votre attaque passe relativement bien à l'échelle.

(Q20) Vous pouvez vous amuser à implémenter une attaque en prenant en compte des permutations de bits, et/ou plus de deux tours de chiffrement.