TD4 - Cryptanalyse Différentielle

Responsable : M. Bombar

1 Un chiffrement par bloc simple

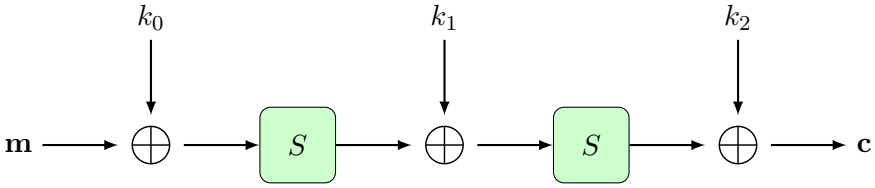

FIGURE 1 – Un chiffrement à deux tours sans permutation

On considère le chiffrement présenté en Figure 1, constitué de deux Sbox de 4 bits dont la table de valeurs est donnée en Figure 1 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.

(Q1) 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.

(Q2) 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.

(Q3) Déterminez la table distribution des différences de S.

(Q4) Quelle est l'uniformité différentielle de S ?

(Q5) Déterminez une caractéristique différentielle pertinente pour la cryptanalyse de ce chiffrement. Quelle est sa probabilité d'apparition ?

a. Ou autre si vous préférez !

1.1 Simplification : Chiffrement à un tour unique

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

(Q6) Décrivez les étapes de la cryptanalyse différentielle de ce système de chiffrement à un tour unique.

(Q7) 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 $\Delta(\mathbf{m}) = \alpha$, $\Delta(\mathbf{c}) = \beta$.

(Q8) 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.

(Q9) 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.

(Q10) Terminez d'implémenter la cryptanalyse différentielle en retrouvant la clé secrète complète. De combien de paires de clairs-chiffrés connus avez-vous besoin ?

(Q11) 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).

1.2 Augmenter le nombre de tours

(Q12) Rappelez le principe de la cryptanalyse différentielle d'un système de chiffrement à plusieurs tours.

(Q13) Implémentez la cryptanalyse différentielle de ce système de chiffrement dans le cas de deux tours.

(Q14) 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.

(Q15) Vérifiez de même que votre attaque passe relativement bien à l'échelle.

(Q16) Vous pouvez vous amuser à implémenter une attaque en prenant en compte des permutations de bits, et/ou plus de deux tours de chiffrement.

2 Challenges

2.1 Chiffrement à un tour

Ce sera un chiffrement à un tour mais avec des boîtes S assez grosses.

2.2 Chiffrement à deux tours

Ils vous faudra retrouver la clé secrète d'un chiffrement à deux tours de la forme décrite dans ce TP.