TD11 - Révisions de Cryptanalyse (Solutions)

Responsable : M. Bombar

1 Introduction

On suppose que les boîtes S sont sur 4 bits par la Table 1

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

TABLE 1 – Représentation de la boîte S (en hexadécimal)

La couche linéaire de diffusion pour chaque tour est une simple permutation linéaire des bits. Elle est représentée graphiquement en Figure 1 ainsi que dans la Table 2.

input	1	2	3	4	5	6	7	8	9	10	11	12	12	14	15	16
output	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

TABLE 2 – Permutation

2 Cryptanalyse Linéaire

2.1 Approximation des boîtes S

On rappelle la définition de la table des approximations linéaires d'une boîte S.

Définition

Pour chaque masque linéaire (α, β), on définit

$$\mathrm{LAT}[\alpha][\beta] = \sigma_{\alpha,\beta} - 2^{n-1} = 2^{n-1}\varepsilon_{\alpha,\beta}.$$

où

$$\sigma_{\alpha,\beta} = \#\Big\{\mathbf{x} \mid \langle\alpha, \mathbf{x}\rangle + \langle\beta, S(\mathbf{x})\rangle = 0\Big\}$$

est le nombre de solutions à l'approximation linéaire et

$$\mathbb{P}_{\mathbf{x}}\Big(\langle\alpha, \mathbf{x}\rangle + \langle\beta, S(\mathbf{x})\rangle = 0\Big) \overset{\text{def}}{=} \frac{\sigma_{\alpha,\beta}}{2^n} = \frac{1}{2}\big(1 + \varepsilon_{\alpha,\beta}\big)$$

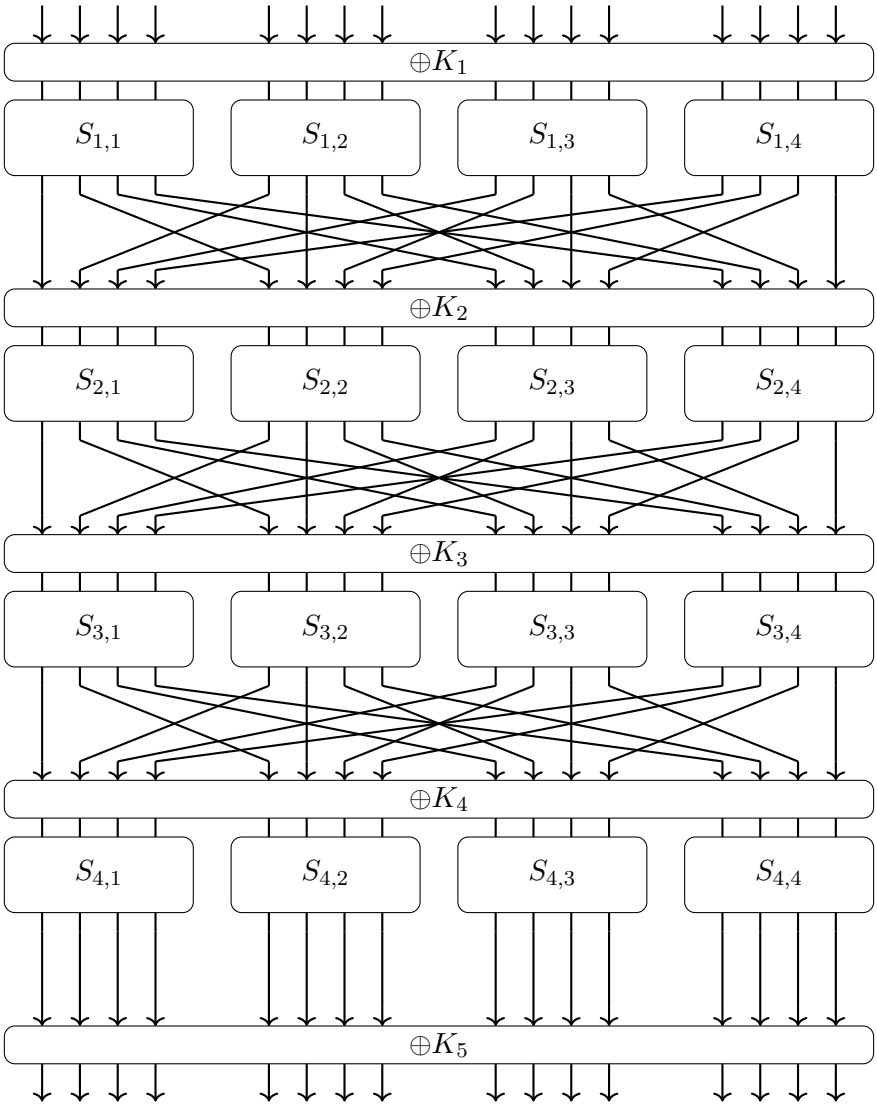


FIGURE 1 – Chiffrement par blocs de type SPN

(Q1) Construire une table des approximations linéaires de S.

(Q2) Quelle est le biais le plus probable ?

(Q3) Donner un masque (α, β) qui l'atteint.

solution

(Q1)

$\alpha \setminus \beta$	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	-2	-2	-	-	-2	6	2	2	-	-	2	2	-	-
2	-	-	-2	-2	-	-	-2	-2	-	-	2	2	-	-	-6	2
3	-	-	-	-	-	-	-	-	2	-6	-2	-2	2	2	-2	-2
4	-	2	-	-2	-2	-4	-2	-	-	-2	-	2	2	-4	2	-
5	-	-2	-2	-	-2	-	4	2	-2	-	-4	2	-	-2	-2	-
6	-	2	-2	4	2	-	-	2	-	-2	2	4	-2	-	-	-2
7	-	-2	-	2	2	-4	2	-	-2	-	2	-	4	2	-	2
8	-	-	-	-	-	-	-	-	-2	2	2	-2	2	-2	-2	-6
9	-	-	-2	-2	-	-	-2	-2	-4	-	-2	2	-	4	2	-2
a	-	4	-2	2	-4	-	2	-2	2	2	-	-	2	2	-	-
b	-	4	-	-4	4	-	4	-	-	-	-	-	-	-	-	-
c	-	-2	4	-2	-2	-	2	-	2	-	2	4	-	2	-	-2
d	-	2	2	-	-2	4	-	2	-4	-2	2	-	2	-	-	2
e	-	2	2	-	-2	-4	-	2	-2	-	-	-2	-4	2	-2	-
f	-	-2	-4	-2	-2	-	2	-	-	-2	4	-2	-2	-	2	-

(Q2) La valeur maximale de la table (en valeur absolue) est 6, qui correspond donc au biais maximal $\frac{6}{2^{4-1}} = \frac{6}{8} = \frac{3}{4}$.

(Q3) Il est atteint par exemple par l'approximation (1, 7).

2.2 Approximation Linéaire du Chiffré

On souhaite maintenant obtenir une approximation linéaire liant le texte clair avec l'entrée du 4ème tour. On souhaite que ça n'active que peu de bits de la clé pour pouvoir bénéficier de l'attaque.

Pour une boîte S donnée, on note X_1, X_2, X_3, X_4 ses entrées et Y_1, Y_2, Y_3, Y_4 ses sorties.

On considère une approximation du chiffrement par blocs faisant intervenir les boîtes $S_{1.2}, S_{2,2}, S_{3,2}$ et $S_{3,4}$.

(Q4) Quelle est la probabilité que $X_1 \oplus X_3 \oplus X_4 = Y_2$ pour $S_{1,2}$?

(Q5) Quelle est la probabilité que $X_2 = Y_2 \oplus Y_4$ pour $S_{2,2}$?

(Q6) Quelle est la probabilité que $X_2 = Y_2 \oplus Y_4$ pour $S_{3,2}$?

solution

On note que les boîtes S sont toutes identiques. Ces approximations se lisent dans la table des approximations linéaires construite dans les questions précédentes. On rappelle que la probabilité qu'une approximation de masque (α, β) apparaisse est

$$\mathbb{P}_{\mathbf{x}}\Big(\langle \alpha, \mathbf{x}\rangle + \langle \beta, S(\mathbf{x})\rangle = 0\Big) = \frac{1}{2}\big(1 + \varepsilon_{\alpha,\beta}\big).$$

où

$$\varepsilon_{\alpha,\beta} = \frac{\mathrm{LAT}[\alpha][\beta]}{2^{n-1}}.$$

(Q4) Cette approximation correspond aux masques $\alpha \overset{\text{def}}{=} (1,0,1,1) = 0\text{xb}$ entrée et $\beta = (0,1,0,0) = 0\text{x4}$ en sortie (puisque $\langle \alpha, \mathbf{X}\rangle = 1\cdot X_1 + 0\cdot X_2 + 1\cdot X_3 + 1\cdot X_4 = X_1 + X_3 + X_4$ et $\langle \beta, \mathbf{Y}\rangle = 0\cdot Y_1 + 1\cdot Y_2 + 0\cdot Y_3 + 0\cdot Y_4 = Y_2$). Dans la table, on lit $\dfrac{\mathrm{LAT}[\alpha][\beta]}{8} = \dfrac{4}{8} = \dfrac{1}{2}$. On en déduit donc que cette approximation est vraie avec probabilité

$$\pi_{\alpha,\beta} = \frac{1}{2}\Big(1 + \frac{1}{2}\Big) = \frac{3}{4}.$$

(Q5) Cette approximation correspond aux masques $\alpha \overset{\text{def}}{=} (0,1,0,0) = 0\text{x4}$ entrée (le masque d'entrée au tour 2 est le masque de sortie au tour 1) et $\beta = (0,1,0,1) = 0\text{x5}$ en sortie. Dans la table, on lit $\mathrm{LAT}[\alpha][\beta] = -4$. On en déduit donc que cette approximation est vraie avec probabilité

$$\pi_{\alpha,\beta} = \frac{1}{2}\Big(1 + \Big(\frac{-4}{8}\Big)\Big) = \frac{1}{2}\Big(1 - \frac{1}{2}\Big) = \frac{1}{4}.$$

(Q6) Même masque que la question précédente, et même boîte S, donc on a la même probabilité.

Pour tout i on note U_i (respectivement V_i) le bloc de 16 bits de l'entrée (resp. de sortie) de la boîte S du tour i, et pour tout j on note $U_{i,j}$ (resp. $V_{i,j}$) le j-ème bit (numeroté de 1 à 16 de gauche à droite). Par exemple, si P désigne le texte clair, on a $U_1 = P \oplus K_1$.

(Q7) Sous l'hypothèse que les approximations linéaires sont indépendantes, démontrer que la relation linéaire

$$V_{2,6} \oplus V_{2,8} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} = 0 \tag{1}$$

se produit avec probabilité $3/8$.

(Q8) Démontrez que

$$V_{3,6} \oplus V_{3,8} = U_{3,6}$$

et

$$V_{3,14} \oplus V_{3,16} = U_{3,14}$$

se produisent toutes les deux avec probabilité $1/4$.

(Q9) Montrer que

$$V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{2,8} \oplus K_{3,14} = 0 \tag{2}$$

avec probabilité $5/8$.

(Q10) En combinant (1) et (2), montrer que

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0$$

avec biais $-1/16$, où

$$\Sigma_K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus K_{4,6} \oplus K_{4,8} \oplus K_{4,14} \oplus K_{4,16}.$$

Puisque les additions de clé ne change pas la magnitude du biais, on en déduit que

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0$$

a lieu avec biais $\pm 1/16$.

solution

(Q7) On suit le chemin linéaire et on regarde la composition des couches 1 et 2. Faites un dessin ! Je l'ai représenté en Figure 2.

— **Couche 1 :** On applique la première approximation avec la boîte $S_{1,2}$

$$V_{1,6} = U_{1,5} \oplus U_{1,7} \oplus U_{1,8}$$

i.e.,

$$V_{1,6} = (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}), \tag{3}$$

qui arrive avec probabilité $3/4$ (biais $+1/2$).

— **Couche 2 :** On applique la deuxième approximation pour la boîte $S_{2,2}$

$$U_{2,6} = V_{2,6} \oplus V_{2,8}$$

qui est vraie avec probabilité $1/4$. Puisque $U_{2,6} = V_{1,6} \oplus K_{2,6}$ on en déduit l'approximation

$$V_{2,6} \oplus V_{2,8} = V_{1,6} \oplus K_{2,6} \tag{4}$$

avec probabilité $1/4$ (biais $-1/2$).

En combinant les équations (3) et (4), on en déduit une approximation linéaire

$$V_{2,6} \oplus V_{2,8} = (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8}) \oplus K_{2,6} \tag{5}$$

ou encore

$$\underbrace{(V_{2,6} \oplus V_{2,8} \oplus K_{2,6})}_{\text{biais } 1/2} \oplus \underbrace{(P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8})}_{\text{biais } -1/2} = 0. \tag{6}$$

Pour calculer la probabilité que cette approximation ait lieu, on utilise évidemment le **Piling-Up Lemma** (Ne réinventez pas la roue ! ! On cherche le biais de la somme de deux variables aléatoires de Bernoulli, qu'on suppose indépendentes) : le biais de cette approximation est le produit des biais. On a donc un biais de $\frac{1}{2} \times \frac{-1}{2} = -\frac{1}{4}$, et donc l'approximation donnée par (6) est vraie avec probabilité

$$\frac{1}{2}\left(1 - \frac{1}{4}\right) = \frac{3}{8}.$$

solution

(Q8) On continue, avec la couche 3 en cherchant des approximations des boîtes $S_{3,2}$ et $S_{3,4}$:

— Pour $S_{3,2}$ on a l'approximation

$$V_{3,6} \oplus V_{3,8} = U_{3,6} \tag{7}$$

avec probabilité $\frac{1}{4}$ (*i.e.*, avec un biais $-1/2$).

— Pour $S_{3,4}$ on a l'approximation

$$V_{3,14} \oplus V_{3,16} = U_{3,14} \tag{8}$$

avec probabilité $\frac{1}{4}$ (*i.e.*, avec un biais $-1/2$).

(Q9) On utilise l'égalité $U_{3,6} = V_{2,6} \oplus K_{3,6}$ et $U_{3,14} = V_{2,8} \oplus K_{3,14}$ (obtenues en suivant la permutation, voir Figure (2)), et on combine les équations (7) et (8). On calcule les probabilités d'apparition à l'aide du **Piling-Up Lemma**. On en déduit que l'approximation suivante

$$\underbrace{\left(V_{3,6} \oplus V_{3,8} \oplus V_{2,6} \oplus K_{3,6}\right)}_{\text{Equation (7), biais } -1/2} \oplus \underbrace{\left(V_{3,14} \oplus V_{3,16} \oplus V_{2,8} \oplus K_{3,14}\right)}_{\text{Equation (8), biais } -1/2} = 0 \tag{9}$$

se produit avec biais $\left(\frac{-1}{2}\right) \times \left(\frac{-1}{2}\right) = \frac{1}{4}$, ou encore que l'équation (9) se produit avec probabilité

$$\frac{1}{2}\left(1 + \frac{1}{4}\right) = \frac{5}{8}.$$

solution

(Q10) On définit les variables aléatoires

$$X_{12} \stackrel{\text{def}}{=} V_{2,6} \oplus V_{2,8} \oplus K_{2,6} \oplus P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8}$$

et

$$X_3 \stackrel{\text{def}}{=} V_{3,6} \oplus V_{3,8} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,8} \oplus K_{3,14}.$$

C'est-à-dire que X_{12} correspond à l'approximation linéaire des couches 1 et 2, tandis que X_3 correspond à l'approximation linéaire de la couche 3. Ce sont deux variables aléatoires de Bernoulli, et les équations (6) et (9) nous disent exactement que

$$\mathbb{P}(X_{12}=0) = \frac{1}{2}\Big(1-\frac{1}{4}\Big) = \frac{3}{8} \quad \text{et} \quad \mathbb{P}(X_3=0) = \frac{1}{2}\Big(1+\frac{1}{4}\Big) = \frac{5}{8}.$$

En supposant encore l'indépendance des tours, le **piling-up lemma** nous dit que $X_{12}+X_3$ est une variable de Bernoulli de biais $(-1/4)\times(1/4) = -1/16$, *i.e.*,

$$\mathbb{P}(X_{12}+X_3=0) = \frac{1}{2}\Big(1-\frac{1}{16}\Big) = \frac{15}{32}.$$

En d'autre termes, on a l'approximation suivante

$$K_{2,6}\oplus P_5\oplus P_7\oplus P_8\oplus K_{1,5}\oplus K_{1,7}\oplus K_{1,8}\oplus V_{3,6}\oplus V_{3,8}\oplus K_{3,6}\oplus V_{3,14}\oplus V_{3,16}\oplus K_{3,14} = 0 \tag{10}$$

avec probabilité $15/32$,*i.e.*, avec biais $-1/16$.

Enfin, on peut utiliser les égalités suivantes (obtenues en suivant la permutation, voir Figure 2) :

- $U_{4,6} = V_{3,6} \oplus K_{4,6}$ *i.e.*, $V_{3,6} = U_{4,6} \oplus K_{4,6}$
- $U_{4,8} = V_{3,14} \oplus K_{4,8}$ *i.e.*, $V_{3,14} = U_{4,8} \oplus K_{4,8}$
- $U_{4,14} = V_{3,8} \oplus K_{4,14}$ *i.e.*, $V_{3,8} = U_{4,14} \oplus K_{4,14}$
- $U_{4,16} = V_{3,16} \oplus K_{4,16}$ *i.e.*, $V_{3,16} = U_{4,16} \oplus K_{4,16}$

et on en déduit que l'approximation

$$U_{4,6} \oplus U_{4,14} \oplus U_{4,8} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K = 0 \tag{11}$$

se produit avec probabilité $15/32$ (*i.e.*, avec biais $-1/16$), où on a posé

$$\Sigma_K \stackrel{\text{def}}{=} K_{4,6} \oplus K_{4,14} \oplus K_{4,8} \oplus K_{4,16} \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14}.$$

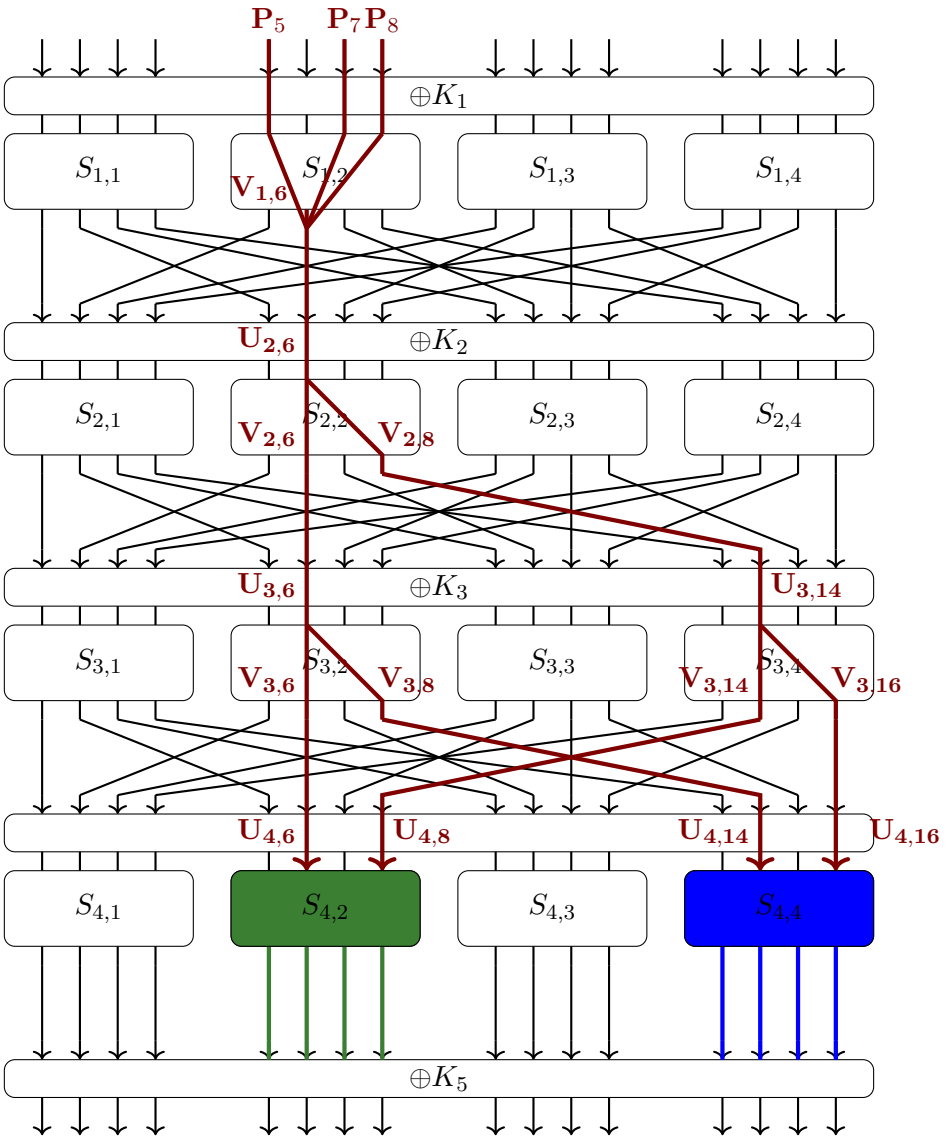


FIGURE 2 – Chemin linéaire que l'on considère pour faire l'approximation

2.3 Extraire les bits de la clé

(Q11) Rappeler comment monter une attaque de dernier tour.

solution

(Q11) Dans une attaque de dernier tour, notre objectif est d'établir un distingueur sur les $R-1$ premiers tours du chiffrement (dans notre cas $R=4$), puis on fait une recherche exhaustive sur les bits de la clé K_{R+1}. Plus précisément, on suppose que l'on dispose de nombreux couples (clair-chiffré) obtenus avec la véritable clé. Pour chaque clé candidate $\widetilde{K_{R+1}}$, on va alors partir de chaque chiffré, et inverser le dernier tour (*i.e.*, on ajoute $\widetilde{K_{R+1}}$, on inverse la couche linéaire (en général l'identité pour le dernier tour), ainsi que les boîtes S). On obtient alors un chiffré intermédiaire potentiel. Si la clé candidate était correcte, on devrait alors observer le biais que l'on a établit.

Par exemple, dans le cadre de cet exercice, l'équation (11) nous dit que les 4 bits $(U_{4,6}, U_{4,8}, U_{4,14}, U_{4,16})$ de chiffré intermédiaire sont en relation avec les bits (P_5, P_7, P_8) de clairs via la relation

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} = P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_K$$

qui se produit avec biais $-1/16$ (où l'aléas est bien entendu pris sur les bits de P). A priori, cette relation dépend des bits de la clé (via Σ_K), qui sont bien sûr inconnus. Néanmoins, ils ne changent pas selon le couple clair-chiffré considéré. En d'autres termes, Σ_K est un **bit constant** (inconnu). Par conséquent, on peut simplifier l'équation précédente pour obtenir une approximation des tours 1 à 3 de la forme suivante

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} = P_5 \oplus P_7 \oplus P_8 \tag{12}$$

avec biais $-1/16$ (dans le cas où $\Sigma_K = 0$), ou avec biais $1/16$ (dans le cas où $\Sigma_K = 1$). En d'autres termes, l'équation (12) se produit avec probabilité

$$\frac{1}{2}\left(1 \pm \frac{1}{16}\right) \in \left\{\frac{15}{32}, \frac{17}{32}\right\}.$$

solution

(suite) Par ailleurs, on observe que cette relation ne fait intervenir que les bits d'entrée des boîtes $S_{4,2}$ et $S_{4,4}$, elles même uniquement connectées aux bits de clé $K_{5,5}, K_{5,6}, K_{5,7}, K_{5,8}, K_{5,13}, K_{5,14}, K_{5,15}$ et $K_{5,16}$. On va alors tester les 256 possibilités, et pour chacune d'entre elles on va initialiser un compteur C_K. Pour chaque paire (P, C) de (clair, chiffré) on va déterminer les bits $U_{4,6}, U_{4,8}, U_{4,14}$ et $U_{4,16}$ correspondant à C. Si on observe le biais, *i.e.*, si l'équation (12) a bien lieu, on va incrémenter C_K. Si la clé est mauvaise, on s'attend à ce que $C_K \approx$ la moitié du nombre de paires. Sinon, l'équation (12) doit avoir lieu plus souvent (biais $1/16 > 0$, ce qui correspond dans notre cas à $\Sigma_K = 1$), ou moins souvent (biais $-1/16$, qui correspond à $\Sigma_K = 0$). Dans les deux cas, la valeur du compteur C_K doit être éloignée de la moitiée dans le cas où le candidat K est correct. On renvoie alors la clé candidate correspondant au compteur le plus éloigné de $1/2$. Si on a N couples (P, C), on renvoie la clé dont le compteur maximise $\dfrac{|C_K - N/2|}{N}$ (qui lui-même doit être proche de $|\varepsilon/2|$, *i.e.*, ici $1/32$). En général, il va nous falloir un nombre N de couples de l'ordre de $\Omega(\varepsilon^2)$ pour que ce distingueur fonctionne. Ici, avec $N \approx 10000$ on doit vraiment bien voir le biais.

3 Exercices sur les fonctions de hachage

3.1 Résistance aux collisions n'implique pas résistance aux préimages

Soit $h : \{0,1\}^\star \to \{0,1\}^n$ une fonction de hachage qu'on suppose **résistante aux collisions**. On construit la fonction de hachage suivante

$$h' : \begin{cases} \{0,1\}^\star & \to & \{0,1\}^{n+1} \\ x & \mapsto & \begin{cases} 0||x & \text{si } |x| = n. \\ 1||h(x) & \text{sinon.} \end{cases} \end{cases}$$

(Q12) Montrez que h' est résistante aux collision.

(Q13) Rappelez la définition formelle de la résistance à la préimage.

(Q14) Montrez que h' n'est pas résistante à la préimage.

solution

(Q12) Soient $x \neq x'$ telles que $h'(x) = h'(x')$. Remarquons qu'aucune des deux ne peut-être de longueur n. En effet, si l'une est de longueur n, sans perte de généralité on peut supposer que c'est x, alors si x' est aussi de longueur n, la collision donne $0||x = 0||x'$ puis $x = x'$. Mais de l'autre côté, si x' n'est pas de longueur n, le hashés commencent par deux bits distincts, donc ne peuvent pas collisionner. Par conséquent, $h'(x) = 1||h(x)$ et $h'(x') = 1||h'(x')$, et on en déduit $h(x) = h(x')$. En d'autres termes, une collision sur h' implique une collision sur h. Comme cette dernière est résistante aux collisions, on en déduit qu'il en est de même pour h' (au sens où trouver une collision pour h' est plus difficile que de trouver une collision pour h).

(Q13) Soit $\mathcal{A}$ un algorithme PPT et $H : \{0,1\}^\star \to \{0,1\}^N$ une fonction de hachage. On note

$$\pi_{\mathcal{A}} \stackrel{\text{def}}{=} \mathbb{P}_y \left(\mathcal{A}(y) = x \text{ et } H(x) = y \right),$$

la probabilité que $\mathcal{A}$ trouve un antécédent par H à $y \leftarrow \{0,1\}^N$ (l'aléas est pris sur le choix de y et l'aléas interne de $\mathcal{A}$). La fonction de hachage H est dite résistante à la préimage si on ne sait pas construire un algorithme PPT $\mathcal{A}$ tel que $\pi_{\mathcal{A}}$ soit non négligeable (en N).

(Q14) Soit $y = (y_0, \ldots, y_n) \leftarrow \{0,1\}^{n+1}$ uniformément distribué. On considère l'algorithme $\mathcal{A}$ suivant :

- Si $y_0 = 0$, alors $\mathcal{A}$ renvoie $y_1, \ldots, y_n$.
- Sinon, $\mathcal{A}$ renvoie 0^n.

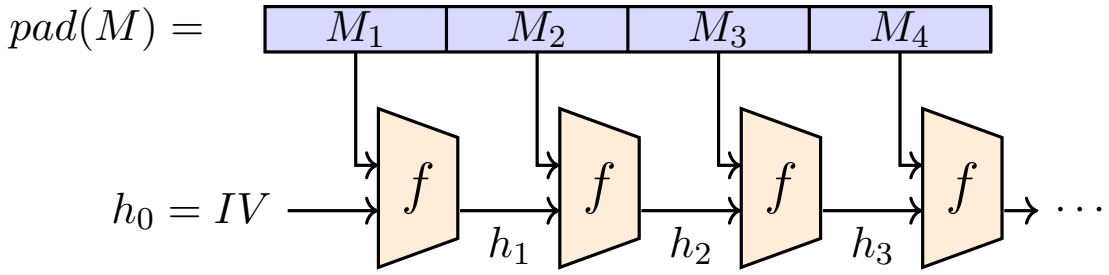
Alors $\mathcal{A}$ est déterministe, et de plus $\mathcal{A}(y)$ est bien une préimage de y par h' si $y_0 = 0$, par définition. Plus formellement, la loi des probabilités totales donne

$$\begin{aligned}
\mathbb{P}_y \left(h'(\mathcal{A}(y)) = y \right) &= \mathbb{P}_y \left(h'(\mathcal{A}(y)) = y \mid y_0 = 0 \right) \mathbb{P}_y(y_0 = 0) \\
&\quad + \mathbb{P}_y \left(h'(\mathcal{A}(y)) = y \mid y_0 = 1 \right) \mathbb{P}_y(y_1 = 0) \\
&= \frac{1}{2} + \frac{1}{2} \underbrace{\mathbb{P}_y((1||y_1, \ldots, y_n) = h'(0^n))}_{=0 \text{ car } h'(0^n) = 0^{n+1}} \\
&= \frac{1}{2}
\end{aligned}$$

qui est bien non négligeable !

3.2 Length-Extension Attack sur la construction de Merkle-Damgård

Soit H une fonction de hachage construite selon la méthode de Merkle-Damgård (par exemple MD5, SHA1, SHA256), dont on rappelle la construction ci-dessous.



(Q15) Soit $h = H(m) \in \{0,1\}^n$ le hash d'un message $m \in \{0,1\}^\star$ considéré comme secret. Soit $\sigma \in \{0,1\}^\star$ un suffixe quelconque (choisi par l'attaquant). Montrez qu'il est possible d'obtenir efficacement le hash d'un message étendu de la forme $m||padding||\sigma$ en temps $O(|\sigma|)$.

Indication : Supposer dans un premier temps que le message est de la bonne longueur, c'est-à-dire qu'il n'y a pas de *padding* interne.

(Q16) On considère un client C et un serveur S ayant partagé une clé secrète sk (par exemple à l'aide d'un protocole d'échange de clés comme celui de Diffie-Hellman). Afin de limiter les attaques de type *Man-in-the-middle* dans la suite du protocole (on suppose que sk n'est pas compromise), on propose de rajouter à chaque message m échangé entre C et S un identifiant supplémentaire de la forme $H(sk||m)$. Ainsi, chaque message échangé entre C et S est maintenant de la forme

m	$H(sk\|\|m)$

Montrez que ce processus n'est absolument pas sécurisé dans le sens où un attaquant peut modifier le message m de sorte à obtenir un paquet valide entre C et S.

solution

(Q15) Par définition, la construction de Merkle-Damgard permet d'obtenir le hash d'un bloc M_{n+1} comme $f(h_n, M_{n+1})$ où h_n est **exactement** le hashé des n premiers blocs ! Il suffit alors de continuer à hasher pour pouvoir étendre un hash déjà connu. Ce processus se fait bien en temps linéaire en le suffixe. Si le suffixe n'est pas déjà de la bonne taille, il faut rajouter un padding, mais celui-ci ne change pas le processus en lui même.

(Q16) On suppose qu'un attaquant intercepte les messages échangés dans le protocole (attaque de type *man-in-the-middle*). Il peut alors aisément rajouter n'importe quel suffixe à m, et modifier le tag grace à l'attaque précédente, et ce, sans même connaître la clé secrète !

Remarque : Exemple d'utilisation récente en pratique pour attaquer le protocole radius utilisé par exemple par Eduroam `https://www.blastradius.fail/`.