Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 3.22

Dans cet exercice, nous allons construire un distingueur pour un système de chiffrement par bloc qui exploite des propriétés arithmétiques de la fonction de tour. Il s'agit du système de chiffrement par bloc M6 proposé pour le standard *IEEE1394 FireWire*. Le chiffrement utilise un schéma de Feistel à 10-tours et chiffre des blocs de 64 bits en utilisant des clés de 64 bits. La fonction de tour F utilisée est définie par $F(x,y) = (y + f(x) \bmod 2^{32}, x)$ avec

$$\begin{array}{ll} g_1(x) = x \oplus K_1 & g_2(y) = (y \lll 2) + y + 1 \bmod 2^{32} \\ g_3(z) = (z \lll 8) + z \bmod 2^{32} & g_4(a) = a + K_2 \bmod 2^{32} \\ g_5(b) = (b \lll 14) + b \bmod 2^{32} & f(x) = (g_5 \circ g_4 \circ g_3 \circ g_2 \circ g_1)(x). \end{array}$$

où $K = (K_1, W) \in \{0,1\}^{64}$ est la clé de 64 bits et $K_2 = K_1 + W \bmod 2^{32}$.

Exercice 3.22 DISTINGUEUR POUR LE CHIFFREMENT M6

1. Montrer que $f(x) \bmod 5 \in \{0,4\}$ pour tout $x \in \{0,1\}^{32}$. Nous admettrons que $f(x) \bmod 5$ est uniformément distribué dans $\{0,4\}$.
2. En déduire que si $F(x,y) = (y',x)$, alors $y' - y \bmod 5 \in \{0,3,4\}$ pour tout $x,y \in \{0,1\}^{32}$ et que les valeurs 0, 3 et 4 sont obtenues avec probabilité $1/4$, $1/4$ et $1/2$ respectivement.
3. En déduire un moyen pour distinguer M6 d'une permutation aléatoire.

Solution :

1. Il suffit de remarquer que $g_5(b) \bmod 5 \in \{0,4\}$. Nous avons

$$g_5(b) = (b \lll 14) + b - 2^{32}k$$

avec $k \in \{0,1\}$ puisque $(b \lll 14) + b < 2^{33}$. Donc

$$g_5(b) = (2^{14}+1)b - 2^{32}k \bmod 2^{32}-1$$

et comme 5 divise $2^{32}-1$, $2^{14}+1 \equiv 0 \bmod 5$ et $2^{32} \equiv 1 \bmod 5$, nous avons

$$g_5(b) \equiv -k \bmod 5,$$

d'où le résultat.

2. Posons $(y',x) = F(x,y) = (y + f(x) \bmod 2^{32}, x)$. Nous avons $y' - y = f(x) \bmod 2^{32}$. Il existe donc $k \in \{-1,0\}$ uniformément distribué tel que

$$y' - y = f(x) + 2^{32}k.$$

En réduisant modulo 5, nous obtenons

$$y' - y \bmod 5 \in \{0,3,4\},$$

avec la distribution suivante :

$f(x)$	0	0	4	4
k	-1	0	-1	0
$y'-y \bmod 5$	4	0	3	4

Donc $y' - y \bmod 5$ prend les valeurs 0, 3 et 4 avec probabilité $1/4$, $1/4$ et $1/2$ respectivement.

3. Posons m^L la partie gauche du clair et c^L la partie gauche du chiffré. La valeur $c^L - m^L$ est la somme de cinq variables aléatoires que nous supposons indépendantes dont la valeur modulo 5 a la distribution $(1/4,0,0,1/4,1/2)$ (puisque le chiffrement M6 est un réseau de Feistel à 10 tours). La distribution de la somme de n variables aléatoires indépendantes modulo 5 dont la distribution est égale à $(1/4,0,0,1/4,1/2)$ est donnée dans le tableau suivant

	0	1	2	3	4
$n=1$	$1/4$	0	0	$1/4$	$1/2$
$n=2$	$1/16$	$1/16$	$1/4$	$3/8$	$1/4$
$n=3$	$7/64$	$15/64$	$5/16$	$15/64$	$7/64$
$n=4$	$57/256$	$35/128$	$57/256$	$9/64$	$9/64$
$n=5$	$127/512$	$55/256$	$165/1024$	$165/1024$	$55/256$

La distribution de $c^L - m^L$ modulo 5 (qui est donc la 5-convolution de la distribution $(1/4,0,0,1/4,1/2)$) vaut approximativement

$$(0,248 \quad 0,215 \quad 0,161 \quad 0,161 \quad 0,215).$$

Un chiffré laisse donc fuir de l'information sur le clair puisque par exemple $c^L \bmod 5$ a environ une chance sur 4 d'être égal à $m^L \bmod 5$ (contre une chance sur 5 pour une permutation aléatoire).

□