Examen Final – Cryptographie

vendredi 18 décembre 2009, 14h – 16h

Documents de cours autorisés

Toutes les réponses doivent être soigneusement justifiées

Exercice 1

1. Calculer la représentation algébrique normale de la fonction booléenne sur $\{0,1\}^3$ suivante

$$f(a,b,c) = (a \vee c) \wedge (c \vee \neg b) \wedge \neg(a \wedge \neg(b \vee c))$$

2. Montrer que le polynôme $P(X) = X^3 + X^2 + 1$ est irréductible sur $\mathbb{F}_2$.

   On travaille dans le corps $\mathbb{F}_{2^3} = \mathbb{F}_2[X]/P(X)$. Un mot de 3 bits $w = a_2a_1a_0$ correspond à un élément $\alpha(w)$ du corps par la correspondance suivante

$$w = a_2a_1a_0 \leftrightarrow \alpha(w) = a_2X^2 + a_1X + a_0 \mod P(X)$$

   Pour deux mots w et v, on définit $w \otimes v$ comme le mot z tel que $\alpha(z) = \alpha(w)\alpha(v)$.

   (a) Calculer $100 \otimes 011$

   (b) Montrer que

$$X(X^2 + X) = 1 \mod P(X)$$

   (c) En déduire que la fonction booléenne vectorielle $G : \{0,1\}^3 \to \{0,1\}^3$ définie par

$$G(w) = 010 \otimes w$$

   est une bijection.

   (d) Calculer la représentation algébrique de G.

3. Construire, à l'aide des fonctions f et G, la représentation normale algébrique d'une fonction booléenne courbe sur $\{0,1\}^6$.

Exercice 2

On considère l'expansion des sous-clés dans A.E.S.

1. Pour $N_k = 4$, calculer l'expression des colonnes C_i, pour $i = 5, ..., 12$, en fonction des colonnes C_1, C_2, C_3, C_4 et des constantes $\texttt{Rcst}_i$.

2. Calculer C_5 en sachant que

$$C_1 = {}^t(\{8E\},\{36\},\{52\},\{1D\}) \quad \text{et} \quad C_4 = {}^t(\{02\},\{3B\},\{B7\},\{39\})$$

Problème 3 (Cryptanalyse linéaire)
On considère le cryptosystème E sur 4 bits donné dans la figure ci-dessous où la S-boîte $\mathcal{S}$ est la suivante (entrée : $x_1x_2x_3x_4$, sortie : $y_1y_2y_3y_4$)

$x_1x_2x_3x_4$	$y_1y_2y_3y_4$	$x_1x_2x_3x_4$	$y_1y_2y_3y_4$	$x_1x_2x_3x_4$	$y_1y_2y_3y_4$	$x_1x_2x_3x_4$	$y_1y_2y_3y_4$
0000	1001	0100	1100	1000	0011	1100	0111
0001	1011	0101	1110	1001	0000	1101	0100
0010	1000	0110	0001	1010	0110	1110	1111
0011	1101	0111	0010	1011	0101	1111	1010

1. Calculer l'image du mot 1101 par le cryptosystème E avec les sous-clés
$$K_1 = K_{1,1}K_{1,2}K_{1,3}K_{1,4} = 1110 \quad \text{et} \quad K_2 = K_{2,1}K_{2,2}K_{2,3}K_{2,4} = 1100$$
2. Déterminer deux sous-clés K_1 et K_2 telles que le cryptage du mot 0110 par le cryptosystème E soit le mot 1010.
3. Soit $y_1y_2y_3y_4 = \mathcal{S}(x_1x_2x_3x_4)$. Déterminer les probabilités suivantes
$$\text{Prob}\big(x_2 = y_2 \oplus y_3 \oplus y_4\big) \text{ et } \text{Prob}\big(x_1 \oplus x_4 = y_3\big)$$
4. En déduire le biais $\varepsilon(\mathcal{S}; u, v) = \varepsilon((\mathcal{S}(x) * v) \oplus (x * u))$ pour
$$(u, v) = (0100, 0111) \quad \text{et} \quad (u, v) = (1001, 0010)$$
Que peut-on en déduire sur la résistance linéaire de la S-boîte $\mathcal{S}$?
5. Déduire de la question (3) deux relations linéaires reliant les bits d'entrées w_1, w_2, w_3, w_4, les bits de sortie w'_1, w'_2, w'_3, w'_4 et les bits des clés K_1 et K_2 qui sont satisfaites avec une forte probabilité.
6. Avec quelles probabilités ses relations sont-elles vérifiées si on remplace $\mathcal{S}$ par une fonction aléatoire sur 4 bits ?
7. Lors d'une attaque à texte clair connue, on observe que, très souvent, on a
$$w_1 \oplus w_4 \neq w'_4$$
Que peut-on en déduire, à l'aide des questions précédentes, sur certains bits des clés K_1 et K_2 ?