Solutions de l'examen final de Cryptographie

vendredi 18 décembre 2009, 14h – 16h

Exercice 1

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

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

Solution. On commence par simplifier l'expression logique

$$\begin{aligned} f(a,b,c) &= (a \vee c) \wedge (c \vee \neg b) \wedge \neg(a \wedge \neg(b \vee c)) \\ &= (a \vee c) \wedge (c \vee \neg b) \wedge (\neg a \vee b \vee c) \\ &= (c \vee (a \wedge \neg b)) \wedge (\neg a \vee b \vee c) \quad \textit{par distributivité} \\ &= c \vee ((a \wedge \neg b) \wedge (\neg a \vee b)) \quad \textit{par distributivité à nouveau} \\ &= c \vee ((a \wedge \neg b) \wedge \neg(a \wedge \neg b)) \\ &= c \end{aligned}$$

Aussi la forme normale de f est X_3 (en prenant $a \rightsquigarrow X_1, b \rightsquigarrow X_2, c \rightsquigarrow X_3$).

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

Solution. On peut regarder les produits possibles entre un polynôme de degré 1 et un polynôme de degré 2 pour voir qu'on n'obtient jamais $P(X)$, et donc qu'il est irréductible. Une autre méthode est de dire que si $P(X)$ est réductible, il est divisible par un polynôme de degré 1 puisqu'il est de degré 3 et donc a une racine dans $\mathbb{F}_2$. Or, $P(0) = P(1) = 1$, donc $P(X)$ est irréductible.

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 $100 \otimes 011$

Solution. On calcule

$$100 \otimes 011 \leftrightarrow X^2(X+1) \mod P(X) = 1 \mod P(X) \leftrightarrow 001$$

(b) Montrer que

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

Solution. (Note : Le calcul est déjà nécessaire pour la question précédente.) On a $X(X^2+X) = X^3 + X^2 = P(X) + 1$ d'où le résultat.

(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.

Solution. On considère l'application $H : \{0,1\}^3 \to \{0,1\}^3$ par $H(w) = 110 \otimes w$. Par la question précédente, on trouve que $H(G(w)) = G(H(w)) = 110 \otimes 010 \otimes w = w$. Donc G admet une fonction réciproque et c'est une bijection.

(d) Calculer la représentation algébrique de G.

Solution. Soit $w = a_2a_1a_0$ un mot de trois bits, on a

$$\begin{aligned} G(w) = 010 \otimes w \leftrightarrow & X(a_2X^2 + a_1X + a_0) \mod P(X) \\ & = a_2X^3 + a_1X^2 + a_0X \mod P(X) = a_2(X^2+1) + a_1X^2 + a_0X \\ & = (a_1 + a_2)X^2 + a_0X + a_2 \\ & \leftrightarrow (a_1 \oplus a_2)a_0a_2 \end{aligned}$$

Donc la représentation algébrique de G est (en prenant $a_0 \rightsquigarrow X_1, a_1 \rightsquigarrow X_2, a_2 \rightsquigarrow X_3$).

$$(X_2 + X_3, X_1, X_3)$$

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

Solution. D'après le cours, puisque G est une permutation, la fonction C définit sur $\{0,1\}^6$ par

$$C(w_1 \cdot w_2) = (w_1 * G(w_2)) \oplus f(w_2)$$

avec $w_1, w_2 \in \{0,1\}^3$, est une fonction courbe. On représente par X_1, X_2, X_3 les bits de w_1 et X_4, X_5, X_6 les bits de w_2. La représentation algébrique de $w_1 * G(w_2)$ est

$$X_1(X_5 + X_6) + X_2X_4 + X_3X_6$$

et donc la représentation algébrique de C est

$$X_1X_5 + X_1X_6 + X_2X_4 + X_3X_6 + X_6$$

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 $\texttt{Rcst}_i$.

Solution. On a

$$\begin{aligned} C_5 &= D_5 \oplus C_1 = \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \\ C_6 &= D_6 \oplus C_2 = C_5 \oplus C_2 = D_5 \oplus C_1 \oplus C_2 = \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \\ C_7 &= D_7 \oplus C_3 = C_6 \oplus C_3 = D_5 \oplus C_1 \oplus C_2 \oplus C_3 = \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \\ C_8 &= D_8 \oplus C_4 = C_7 \oplus C_4 = D_5 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4 \\ &= \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4 \\ C_9 &= D_9 \oplus C_5 = \texttt{SubWord}(\texttt{RotWord}(C_8)) \oplus \texttt{Rcst}_2 \oplus D_5 \oplus C_1 \\ &= \texttt{SubWord}(\texttt{RotWord}(\texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4)) \\ &\quad \oplus \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus \texttt{Rcst}_2 \oplus C_1 \\ C_{10} &= D_{10} \oplus C_6 = C_9 \oplus C_6 = \texttt{SubWord}(\texttt{RotWord}(C_8)) \oplus \texttt{Rcst}_2 \oplus C_5 \oplus C_6 \\ &= \texttt{SubWord}(\texttt{RotWord}(\texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4)) \oplus \texttt{Rcst}_2 \oplus C_2 \\ C_{11} &= D_{11} \oplus C_7 = C_{10} \oplus C_7 \\ &= \texttt{SubWord}(\texttt{RotWord}(\texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4)) \\ &\quad \oplus \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus \texttt{Rcst}_2 \oplus C_1 \oplus C_3 \\ C_{12} &= D_{12} \oplus C_8 = C_{11} \oplus C_8 \\ &= \texttt{SubWord}(\texttt{RotWord}(\texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4)) \\ &\quad \oplus \texttt{Rcst}_2 \oplus C_2 \oplus C_4 \end{aligned}$$

2. Calculer C_5 en sachant que

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

Solution. On a

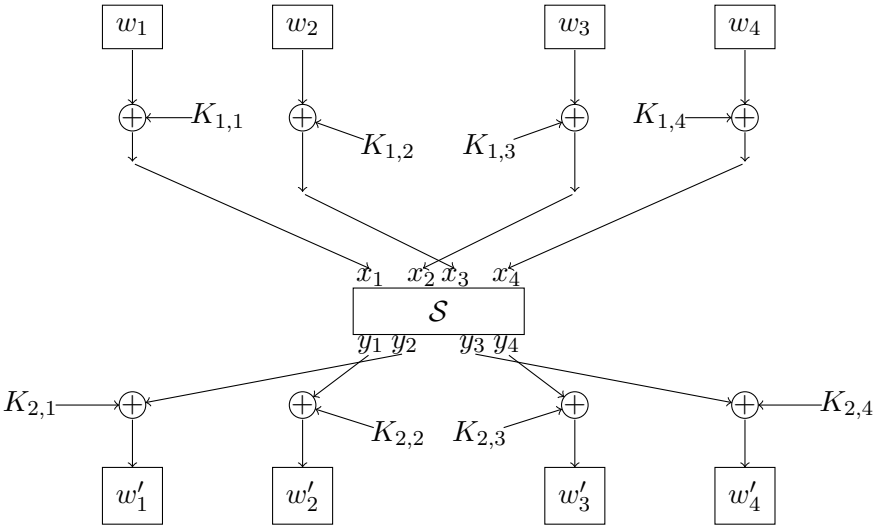
$$\texttt{SubWord}(\texttt{RotWord}(C_4)) = \texttt{SubWord}({}^t(\{3B\},\{B7\},\{39\},\{02\})) = {}^t(\{E2\},\{A9\},\{12\},\{77\})$$

et donc

$$\begin{aligned} C_5 &= \texttt{SubWord}(\texttt{RotWord}(C_4)) \oplus \texttt{Rcst}_1 \oplus C_1 \\ &= {}^t(\{E2\},\{A9\},\{12\},\{77\}) \oplus {}^t(\{01\},\{00\},\{00\},\{00\}) \oplus {}^t(\{8E\},\{36\},\{52\},\{1D\}) \\ &= {}^t(\{6D\},\{9F\},\{40\},\{6A\}) \end{aligned}$$

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

$$K_1 = K_{1,1}K_{1,2}K_{1,3}K_{1,4} = 1110 \quad \text{et} \quad K_2 = K_{2,1}K_{2,2}K_{2,3}K_{2,4} = 1100$$

Solution. On trouve 0101 *à l'entrée de la S-boîte, puis* 1110 *à la sortie et donc l'image est* 0001.

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.

Solution. En fait, on peut choisir ce qu'on veut pour K_1, par exemple $K_1 = 0000$. Donc on a 0110 *avec la S-boîte, puis* 0001 *en sortie. On détermine K_2 de telle sorte que $K_2 \oplus 0010 = 1010$. On trouve $K_2 = 1000$.*

3. Soit $y_1y_2y_3y_4 = \mathcal{S}(x_1x_2x_3x_4)$. Déterminer les probabilités suivantes

$$\mathrm{Prob}\big(x_2 = y_2 \oplus y_3 \oplus y_4\big) \text{ et } \mathrm{Prob}\big(x_1 \oplus x_4 = y_3\big)$$

Solution. On compte le nombre de couples $(x_1x_2x_3x_4, y_1y_2y_3y_4)$ *tels que les égalités soient vérifiées. On en déduit*

$$Prob\big(x_2 = y_2 \oplus y_3 \oplus y_4\big) = \frac{14}{16} = \frac{7}{8}$$

$$Prob\big(x_1 \oplus x_4 = y_3\big) = \frac{14}{16} = \frac{7}{8}$$

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 $\mathcal{S}$?

Solution. On a

$$\varepsilon(\mathcal{S}; 0100, 0111) = Prob\big(x_2 \oplus y_2 \oplus y_3 \oplus y_4 = 0\big) - \frac{1}{2} = \frac{3}{8}$$

$$\varepsilon(\mathcal{S}; 1001, 0010) = Prob\big(x_1 \oplus x_4 \oplus y_3 = 0\big) - \frac{1}{2} = \frac{3}{8}$$

On a déduit que la résistance linéaire de $\mathcal{S}$ *est au plus* 2. (*En fait, elle est égale à* 2.)

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.

Solution. En exprimant les x_i *et les* y_i *en fonctions des* w_i*, des* w'_i *et des* $K_{j,i}$*, on obtient par la question* (3)

$$Prob\big(w_3 \oplus K_{1,3} = w'_1 \oplus w'_3 \oplus w'_4 \oplus K_{2,1} \oplus K_{2,3} \oplus K_{2,4}\big) = \frac{7}{8}$$

$$Prob\big(w_1 \oplus w_4 \oplus K_{1,1} \oplus K_{1,4} = w'_4 \oplus K_{2,4}\big) = \frac{7}{8}$$

6. Avec quelles probabilités ses relations sont-elles vérifiées si on remplace $\mathcal{S}$ par une fonction aléatoire sur 4 bits ?

Solution. Il y deux valeurs possibles équiprobables, donc ces probabilités sont de $1/2$.

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 ?

Solution. Dans la plupart des cas, on doit avoir $w_1 \oplus w_4 \oplus K_{1,1} \oplus K_{1,4} = w'_4 \oplus K_{2,4}$ *par la question* (5)*. Donc, très vraisemblablement, on a* $K_{1,1} \oplus K_{1,4} \neq K_{2,4}$.