Master CSI 2 2010-2011

Cryptanalyse — MHT912

Responsable : G. Castagnos

Examen — mardi 14 décembre 2010, 14h

Durée 3h
Notes de cours autorisées
Nombre de pages : 4
Les 3 exercices sont indépendants

Exercice 1. Fonctions booléennes et boîte S de l'AES

Dans l'AES, on utilise le corps à 256 éléments, $\mathbb{F}_{2^8}$, dans la représentation $\mathbb{F}_{2^8} = \mathbb{F}_2[\alpha]$, avec $\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$, ce qui définit une identification entre $\mathbb{F}_{2^8}$ et $\mathbb{F}_2^8$:

$$\begin{aligned} \mathbb{F}_2^8 &\to \mathbb{F}_{2^8} \\ x = (x_1, \ldots, x_8) &\to x_1 + x_2\alpha + \cdots + x_8\alpha^7 \end{aligned}$$

que l'on utilisera dans la suite. Par cette identification, on définit l'application I :

$$\begin{aligned} I : \mathbb{F}_2^8 &\to \mathbb{F}_2^8 \\ x \mapsto I(x) &= \begin{cases} 0 \text{ si } x = 0 \\ x^{-1} \text{ si } x \neq 0 \end{cases} \end{aligned}$$

où l'inversion x^{-1} est celle du corps $\mathbb{F}_{2^8}$. On rappelle que la boîte S de l'AES est de la forme $S : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ avec $S(x) = A\,I(x) + B$ où A est une certaine matrice carrée 8×8 sur $\mathbb{F}_2$ et B est un certain vecteur 8×1 de $\mathbb{F}_2$.

Pour toute application $T : \mathbb{F}_2^8 \to \mathbb{F}_2^8$,

$$\begin{aligned} T : \mathbb{F}_2^8 &\longrightarrow \mathbb{F}_2^8 \\ x = (x_1, \ldots, x_8) &\longmapsto T(x) = y = (y_1, \ldots, y_8) \end{aligned}$$

on note pour $i = 1, \ldots, 8$, $T_i : x = (x_1, \ldots, x_8) \in \mathbb{F}_2^8 \mapsto y_i \in \mathbb{F}_2$ les 8 applications coordonnées qui sont des fonctions booléennes. On va étudier le degré de ces fonctions booléennes dans le cas de la boîte S de l'AES.

(a) Rappeler la définition du degré d'une fonction booléenne.

(b) Rappeler pourquoi l'application

$$\begin{aligned} \mathbb{F}_2^8 &\longrightarrow \mathbb{F}_2^8 \\ x &\longmapsto x^2 \end{aligned}$$

où le carré est effectué dans $\mathbb{F}_{2^8}$ est linéaire. Écrire sa matrice L dans la base $(1, \alpha, \ldots, \alpha^7)$ (c'est à dire la matrice exprimant en colonne les images de $1, \alpha, \ldots, \alpha^7$ dans la base $(1, \alpha, \ldots, \alpha^7)$).

(c) En déduire l'expression des fonctions coordonnées T_i associées à $T(x) = x^2$. Quel est leur degré ?

(d) Montrez que $x \to x^{2^s}$ est linéaire pour tout entier s. Quelle est sa matrice en fonction de L ?

(e) En déduire que le degré des fonctions coordonnées T_i associées à $T(x) = x^{2^s}$ vaut 1.

(f) Montrez que $I(x) = x^{2^8-2} = x^{2^7+2^6+2^5+2^4+2^3+2^2+2}$.

(g) En déduire le degré des fonctions booléennes coordonnées associées à $I(x)$ puis à $S(x)$.

(h) Quel est, en fonction de u, le degré des fonctions coordonnées associées à $T_u(x) = x^u$ dans $\mathbb{F}_2^8$? Que pensez vous du choix fait pour la puissance de la boîte S de l'AES ?

Exercice 2. Cryptanalyse différentielle d'un schéma S/P

On s'intéresse à un chiffrement par blocs de 16 bits, de type S/P à 2 tours employant 3 clefs K_0, K_1, K_2 de 16 bits. L'étape de substitution utilise 4 fois la même boîte S de 4 bits vers 4 bits donnée par le tableau :

Entrée	Sortie	Entrée	Sortie	Entrée	Sortie	Entrée	Sortie
0000	1110	0100	0010	1000	0011	1100	0101
0001	0100	0101	1111	1001	1010	1101	1001
0010	1101	0110	1011	1010	0110	1110	0000
0011	0001	0111	1000	1011	1100	1111	0111

La permutation s'applique sur les 16 bits de l'état, elle est définie par le tableau suivant (il faut comprendre que le bit d'indice $i \in \{1, \ldots, 16\}$ est envoyé à l'indice $P(i)$).

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$P(i)$	8	7	11	3	15	13	5	16	14	2	9	10	6	4	1	12

Si m est un message clair, on note comme d'habitude $x_0 = m + K_0$ l'entrée du premier tour et x_1 l'entrée du second tour.

(a) Faire un schéma du système de chiffrement (on ne demande pas de représenter précisément la permutation). Pourquoi le système commence par une étape initiale d'ajout de la clef K_0 avant d'effectuer les deux tours ? Rappeler brièvement à quoi sert l'alternance des opérations de substitutions et de permutations.

(b) Donner l'ensemble des couples $(x, x^*) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4$ tels que $x + x^* = 0101$ et $S(x) + S(x^*) = 0001$. D'autre part, on admet qu'il y a 4 couples $(x, x^*) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4$ tels que $x + x^* = 1001$ et $S(x) + S(x^*) = 0111$.

(c) En déduire la probabilité $\text{Prob}[S(x) + S(x^*) = 0001 | x + x^* = 0101]$ et la probabilité $\text{Prob}[S(x) + S(x^*) = 0111 | x + x^* = 1001]$.

(d) Que vaudrait ces probabilités si on remplaçait S par une fonction aléatoire de 4 bits vers 4 bits ? Que peut on dire des probabilités trouvées précédemment pour faire une cryptanalyse différentielle ?

(e) On suppose que l'on prend deux messages clairs m et m^* tels que $m + m^* = 0101\,0000\,0000\,0000$. Que peut on dire de la valeur de la différence $x_1 + x_1^*$ à l'entrée du deuxième tour ? Pourquoi ? Mêmes questions avec la différence $m + m^* = 1001\,0000\,0000\,0000$.

(f) Décrire en détails la cryptanalyse différentielle visant à retrouver la clef K_2 en utilisant la différentielle $x + x^* = 0101, S(x) + S(x^*) = 0001$ (bien préciser les différences de 16 bits sur les messages clairs en entrée, les boîtes actives au dernier tour, les bits de clefs trouvées). Quelle est la complexité minimale de cette attaque pour retrouver tous les bits de K_2 ?

(g) Mêmes questions que **(f)** avec la différentielle $x + x^* = 1001, S(x) + S(x^*) = 0111$.

(h) Entre **(f)** et **(g)**, quelle est l'attaque la plus performante ? Plus généralement, si on utilise une différentielle (α, β) telle que $x + x^* = \alpha$ et $S(x) + S(x^*) = \beta$, que faut il comme propriétés sur β pour avoir une attaque efficace sur ce schéma (en dehors des considérations de probabilités) ?

(i) Décrire brièvement comment on procéderait pour une cryptanalyse différentielle sur ce chiffrement par blocs étendu à 3 tours, dans le but de retrouver la clef du troisième tour, K_3. Quels problèmes pourrait on rencontrer ?

Exercice 3. *Alternating Step Generator*

On considère une variante de l'*Alternating Step Generator*, un chiffrement à flot synchrone additif proposé par Günther en 1987. Ce système utilise trois LFSR : LFSR_X, LFSR_Y et LFSR_C, de longueurs respectives L_X, L_Y et L_C. L'état initial des trois LFSR constitue la clef secrète de

$L_X + L_Y + L_C$ bits. La rétroaction de ces trois LFSR est publique. On suppose que les trois LFSR engendrent des m-suites.

Le LFSR_C est mis à jour à chaque tour et sa sortie est utilisée pour contrôler la mise à jour des deux autres LFSR. La sortie de l'*Alternating Step Generator* est la somme de la sortie des LFSR_X et LFSR_Y.

Plus précisément, le générateur fonctionne comme suit : à chaque instant le LFSR_C est mis à jour,

- Si le bit de sortie du LFSR_C est 0 alors le LFSR_X est mis à jour normalement, et sort un bit noté x. Le LFSR_Y n'est pas mis à jour. On note y le bit qu'il avait sorti lors de sa dernière mise à jour. Le bit de sortie de l'*Alternating Step Generator* est $x + y \mod 2$;
- Sinon, si le bit de sortie du LFSR_C est 1 alors c'est le LFSR_X qui est inchangé, on note x le bit sorti lors de sa dernière mise à jour. Le LFSR_Y est mis à jour et son bit de sortie est noté y. Le bit de sortie de l'*Alternating Step Generator* est toujours $x + y \mod 2$.

Au premier tour, on pose que le bit sorti par les LFSR_X et LFSR_Y lors de leur « dernière » mise à jour vaut 0.

On suppose que l'on a accès aux bits de sortie de l'*Alternating Step Generator*. Proposer une attaque détaillée sur ce générateur visant à retrouver la clef secrète. On précisera en particulier la complexité de l'attaque et le nombre de bits de sortie nécessaires. Que doit on prendre comme taille de paramètres pour se mettre à l'abri de cette attaque ?