Master CSI 2 2013-2014

Cryptanalyse — M1MA9W06
Responsable : G. Castagnos

Examen — mardi 17 décembre 2013

Durée 3h
Documents non autorisés
Nombre de pages : 4
Les 4 exercices sont indépendants

1 Construction de fonction de hachage et fonction de compression

Dans cet exercice, on note comme d'habitude par || la concaténation de deux chaînes de bits, et par $\oplus$ l'addition bit à bit modulo 2 de deux chaînes de bits.

(a) On note f une fonction dite de compression de $\{0,1\}^{n+k}$ dans $\{0,1\}^n$, avec n et k deux entiers strictement positifs. Rappeler la construction de Merkle-Damgård qui permet de construire à partir d'une telle fonction f une fonction de hachage h de $\{0,1\}^*$ dans $\{0,1\}^n$. Si f est résistante aux collisions, que peut on dire de h ? Rappeler la démonstration de ce résultat.

(b) On note dans la suite de l'exercice, $\mathsf{Encrypt}_{sk}(m) = c$ un chiffrement par bloc prenant en entrée un clair m de n bits et une clef sk de k bits et produisant un chiffré c de n bits. Montrer que les trois fonctions de compression f_1, f_2 et f_3 suivantes ne sont pas à sens-unique :
- f_1 qui a une chaîne de bits $m \in \{0,1\}^k$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_1(m||z) = \mathsf{Encrypt}_m(z)$
- f_2 qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_2(m||z) = \mathsf{Encrypt}_z(m) \oplus z$, en supposant $n = k$
- f_3 qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_3(m||z) = \mathsf{Encrypt}_z(z) \oplus m$, en supposant $n = k$

(c) Ces fonctions sont elles résistantes aux collisions ?

(d) On considère maintenant la fonction de compression f qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^k$ associe $f(m||z) = \mathsf{Encrypt}_z(m) \oplus m$. On note pour toute chaîne de bits x, $\overline{x} = x \oplus (11\ldots1)$, la chaîne de bits de même longueur que x constituée des bits complémentaires de ceux de x. On suppose de plus que le chiffrement par bloc vérifie la propriété suivante : $\mathsf{Encrypt}_{\overline{z}}(\overline{m}) = \overline{\mathsf{Encrypt}_z(m)}$ pour tout $m \in \{0,1\}^n$ et $z \in \{0,1\}^k$. Montrer que f n'est pas résistante aux collisions.

2 Suite et polynôme de rétroaction minimal

Dans tout l'exercice on note $z = (z_t)_{t \geqslant 0}$, une suite de bits, et $Z(X)$ sa série génératrice définie par $Z(X) = \sum_{t \geqslant 0} z_t X^t$.

(a) Soit $f(X) \in \mathbf{F}_2[X]$ un polynôme de degré ℓ avec $f(X) = 1 + c_1 X + c_2 X^2 + \cdots + c_\ell X_\ell$. Rappeler sans démonstration la formule reliant $Z(X)$ et $f(X)$ pour que la suite z soit produite par un LFSR de polynôme de rétroaction $f(X)$.

(b) On suppose que z est périodique de période T. Montrer que $X^T Z(X) = Z(X) + \sum_{i=0}^{T-1} z_i X^i$. En déduire le polynôme de rétroaction d'un LFSR permettant d'engendrer Z ainsi qu'une méthode pour déterminer le polynôme de rétroaction minimal d'une suite binaire périodique.

(c) On suppose que z est une m-suite de complexité linéaire ℓ. Comparer l'efficacité de la méthode de la question précédente avec la méthode vue en cours pour trouver le polynôme de rétroaction minimal de z (on rappelle que le calcul du pgcd de deux polynômes de $\mathbf{F}_2$ de degrés inférieurs à e peut être effectué en $\mathcal{O}(e \log^2 e \log\log e)$ opérations dans $\mathbf{F}_2$).

3 Cryptanalyse différentielle d'un schéma Substitution/Permutation.

Dans cet exercice on note comme d'habitude par $\oplus$ l'addition bit à bit modulo 2 de deux chaînes de bits.

On s'intéresse à un chiffrement par blocs de 16 bits, de type Substitution/Permutation à 2 tours employant 3 clefs de tour 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

Le chiffrement se déroule en suivant la construction générale Substitution/Permutation de manière similaire au chiffrement B32 vu en TP. Pour rappel, si m est un message clair, on effectue une étape initiale d'ajout de la première clef de tour : $x_0 = m \oplus K_0$. Puis, on effectue deux tours : pour $i \in \{1, 2\}$ on applique la boîte S sur x_{i-1} découpé en 4 sous blocs de 4 bits, pour donner un nouveau bloc u_i de 16 bits en concaténant les 4 sorties. Puis on applique la permutation P sur les bits de u_i, on note v_i le résultat. Enfin, on ajoute la clef de tour : $x_i = v_i \oplus K_i$. Au bout des deux tours, on obtient le chiffré $c = x_2$.

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

(c) Pour $\alpha, \beta \in \mathbf{F}_2^4$, on note $p_{\alpha,\beta} = \Pr\big[S(x) \oplus S(x^*) = \beta \mid x \oplus x^* = \alpha\big]$, la probabilité que $S(x) \oplus S(x^*) = \beta$ sachant que $x \oplus x^* = \alpha$. Montrer que

$$p_{\alpha,\beta} = \frac{\mathrm{Card}\big\{(x, x^*) \in \mathbf{F}_2^4 \times \mathbf{F}_2^4 \mid x \oplus x^* = \alpha \text{ et } S(x) \oplus S(x^*) = \beta\big\}}{2^4}.$$

En déduire les probabilités $p_{0101,0001} = \Pr[S(x) \oplus S(x^*) = 0001 | x \oplus x^* = 0101]$ et $p_{1001,0111} = \Pr[S(x) \oplus S(x^*) = 0111 | x \oplus x^* = 1001]$.
Intuitivement, que vaudrait ces probabilités si on remplaçait S par une fonction aléatoire de 4 bits vers 4 bits ?

(d) On suppose que l'on prend deux messages clairs m et m^* tels que

$$m \oplus m^* = 0101\,0000\,0000\,0000.$$

Que peut on dire de la valeur de la différence $x_1 \oplus x_1^*$ à l'entrée du deuxième tour ? Bien détailler la probabilité de l'évolution de la différence entre le chiffrement de m et celui de m^* au travers de toutes les étapes jusqu'à l'entrée du deuxième tour. Mêmes questions avec la différence $m \oplus m^* = 1001\,0000\,0000\,0000$.

(e) Un attaquant effectue la cryptanalyse différentielle de ce chiffrement. Pour cela, lors d'une attaque à clairs choisis, il récupère un grand nombre de couples clairs chiffrés, (m, c) et (m^*, c^*) tel que $m \oplus m^* = 0101\,0000\,0000\,0000$. À partir de deux chiffrés c, c^* issus de ces couples, quels bits de K_2 doit il connaître afin de calculer la valeur de $x_1 \oplus x_1^*$ et vérifier si elle correspond à la valeur trouvée à la question précédente ? En déduire un algorithme (en pseudo-code) lui permettant de retrouver ces bits de clefs. Comment pourrait il trouver les autres bits de K_2 ?

(f) Détailler comme l'attaquant pourrait effectuer la même attaque que précédemment en utilisant la différentielle $x \oplus x^* = 1001, S(x) \oplus S(x^*) = 0111$.

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

4 Soit $a, b, \mathrm{K} \in \mathbf{N}^*$, des entiers positifs non nuls. Soit M un entier tel que $a < \mathrm{M}$ et $b < \mathrm{M}$. On considère le réseau $\mathscr{L}$ de $\mathbf{R}^3$ de base

$$\begin{pmatrix} 1 & 0 & \mathrm{K}a \\ 0 & 1 & \mathrm{K}b \end{pmatrix}.$$

(a) Soit $v = (v_1, v_2, v_3)$ un vecteur de $\mathscr{L}$. Montrer que si v_3 est non nul alors $||v|| \geqslant \mathrm{K}$.

(b) Soit b_1 le premier vecteur d'une base LLL réduite. On rappelle que $||b_1|| \leqslant \sqrt{2}||v||$ pour tout $v \in \mathscr{L}$. Montrer que $||b_1|| \leqslant 2\mathrm{M}$.

(c) On suppose $\mathrm{K} > 2\mathrm{M}$. En utilisant le fait que la réduction agit sur la base du réseau par des opérations élémentaires, montrer que la base LLL réduite de $\mathscr{L}$ est de la forme

$$\begin{pmatrix} x_1 & x_2 & 0 \\ u & v & \pm \mathrm{K}g \end{pmatrix}$$

où $g = \mathrm{pgcd}(a, b) = ua + vb$.