Master CSI 2 2020-2021

Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

Examen — mardi 15 décembre 2020

Durée 3h
Documents non autorisés
Les exercices sont indépendants

$\boxed{1}$ Soit $a, b, \mathrm{K}, \mathrm{M} \in \mathbf{N}^*$, des entiers positifs non nuls tels que $a < \mathrm{M}$ et $b < \mathrm{M}$. On considère le réseau $\mathscr{L}$ de $\mathbf{R}^3$ de base donnée par les lignes de la matrice suivante

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

(a) Soit $w = (w_1, w_2, w_3)$ un vecteur de $\mathscr{L}$. Montrer que si w_3 est non nul alors $\|w\| \geqslant \mathrm{K}$.

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

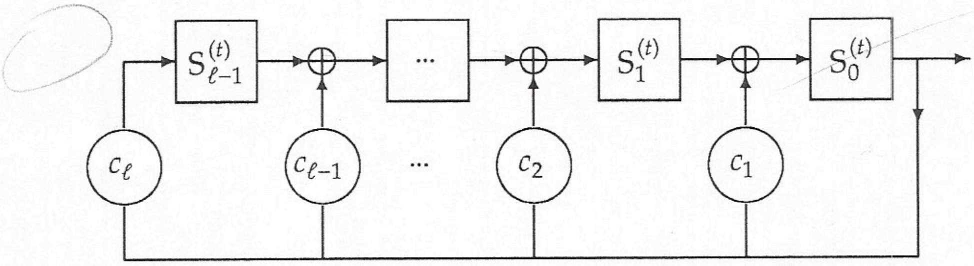
$$\begin{pmatrix} x_1 & x_2 & 0 \\ u & v & \pm \mathrm{K}g \end{pmatrix}$$

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

$\boxed{2}$ Soit $f(\mathrm{X}) \in \mathbf{F}_2[\mathrm{X}]$ un polynôme de degré ℓ avec $f(\mathrm{X}) = 1 + c_1\mathrm{X} + \cdots + c_\ell \mathrm{X}_\ell$. On considère un automate constitué d'un registre de ℓ bits et produisant une suite de bits. On note $\mathrm{S}^{(t)} = (\mathrm{S}_0^{(t)}, \mathrm{S}_1^{(t)}, \dots, \mathrm{S}_{\ell-1}^{(t)})$ l'état du registre à l'instant $t \geqslant 0$. À l'instant t, on sort le bit d'indice 0 du registre, $\mathrm{S}_0^{(t)}$, et on met à jour l'état du registre de la façon suivante (calculs dans $\mathbf{F}_2$) :

$$\mathrm{S}_i^{(t+1)} = \mathrm{S}_{i+1}^{(t)} + c_{i+1}\mathrm{S}_0^{(t)}, \text{ pour } 0 \leqslant i \leqslant \ell - 2 \text{ et } \mathrm{S}_{\ell-1}^{(t+1)} = c_\ell \mathrm{S}_0^{(t)}$$

Le polynôme $f(\mathrm{X})$ est son polynôme de rétroaction. On représente l'automate par le schéma suivant :



(a) Donner les 5 premiers bits produits par cet automate dans le cas $\ell = 3$, avec le polynôme de rétroaction $1 + X + X^3$ de registre initial $S^{(0)} = (S_0^{(0)}, S_1^{(0)}, S_2^{(0)}) = (1,1,0)$.

1 1 0 . . . . .

(b) On considère maintenant le cas général. Pour tout entier t, on désigne par $S^{(t)}(X)$ le polynôme de $\mathbf{F}_2[X]$ de degré au plus $\ell - 1$ correspondant au registre au temps t : c'est à dire $S^{(t)}(X) = S_0^{(t)} + S_1^{(t)}X + \cdots + S_{\ell-1}^{(t)}X^{\ell-1}$. On note z_t le bit sorti au temps t (c'est à dire $S_0^{(t)}$).

Montrer que pour tout entier $t \geqslant 0$, $X \times S^{(t+1)}(X) = S^{(t)}(X) + z_t \times f(X)$.

(c) On note $Z^{(0)}(X) = 0$ et pour tout $t \geqslant 1$, $Z^{(t)}(X) := z_0 + z_1X + \cdots + z_{t-1}X^{t-1}$. Montrer que pour tout $t \geqslant 0$, $S^{(0)}(X) = f(X) \times Z^{(t)}(X) + X^t \times S^{(t)}(X)$.

(d) On note $Z(X)$ la série génératrice de la suite produite par cet automate, c'est à dire que $Z(X) = \sum_{t\geqslant 0} z_tX^t$. Déduire de la question précédente que $Z(X) = S^{(0)}(X)/f(X)$. Montrer que toute suite récurrente linéaire produite par un LFSR peut l'être par cet automate et réciproquement.

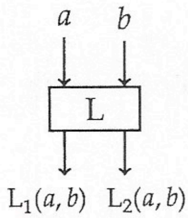
(e) Soit $z = (z_t)_{t\geqslant 0}$ la suite produite par cet automate avec les paramètres de la question (a). Quel LFSR permet de produire la même suite z ? Avec quelle initialisation ? Réciproquement, soit $s = (s_t)_{t\geqslant 0}$ la suite produite par un LFSR de longueur 4, de polynôme de rétroaction $1+X^3+X^4$, initialisé par $(1,1,1,1)$. Quel polynôme de rétroaction et quelle initialisation choisir pour que l'automate de cet exercice produite la même suite s ?

(f) Pour des implantations matérielles on préfère parfois représenter les LFSR comme introduit dans cet exercice plutôt qu'en mode classique. Pourquoi ?

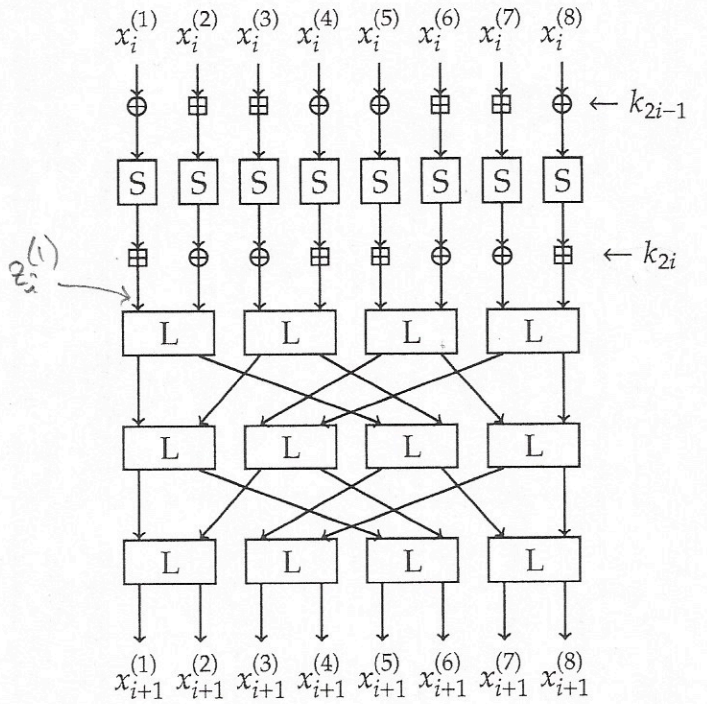
$\boxed{3}$ On considère un chiffrement par bloc itératif. Il chiffre des blocs de 64 bits. L'état interne est également de 64 bits, vus comme 8 octets, chaque octet étant identifié avec un entier de l'ensemble $I := \{0, 1, \ldots, 255\}$. Si x est un bloc de 64 bits, on note $x^{(1)}, x^{(2)}, \ldots, x^{(8)}$ ces 8 octets. Le tour i avec $1 \leqslant i \leqslant 6$ fait intervenir deux sous clefs k_{2i-1} et k_{2i}, de 64 bits. L'addition des clefs avec l'état interne se fait au niveau de chacun des 8 octets, soit par ou exclusif, noté $\oplus$, soit par l'addition modulo 256, notée $\boxplus$. On désigne par S une permutation fixée de l'ensemble I, et par L la fonction de $I \times I \to I \times I$:

$$(a,b) \mapsto (L_1(a,b), L_2(a,b)) := (2a + b \mod 256,\ a + b \mod 256).$$

Cette fonction prend donc deux octets en entrée et ressort deux octets. On la schématise par



Le tour i transforme un bloc de 64 bit x_i en un bloc de 64 bits x_{i+1} par le schéma suivant :



$k_{2i}^{(1)} = k_{2i}^{(2)}$?

On note u_i le bloc de 64 bits après l'application des fonctions S, c'est à dire $u_i^{(1)} = \mathrm{S}(x_i^{(1)} \oplus k_{2i-1}^{(1)})$, $u_i^{(2)} = \mathrm{S}(x_i^{(2)} \boxplus k_{2i-1}^{(2)})$, ... De même, on note z_i le bloc de 64 bits après l'ajout de la clef k_{2i}, c'est à dire $z_i^{(1)} = k_{2i}^{(1)} \boxplus u_i^{(1)}$, $z_i^{(2)} = k_{2i}^{(2)} \oplus u_i^{(2)}$, ...

Le chiffrement complet prend en entrée un message clair $m = x_1$ de 64 bits et retourne un chiffré c de 64 bits obtenu en effectuant 6 tours comme ci dessous avec des clefs $k_1, k_2, \dots, k_{11}, k_{12}$, puis on ajoute à x_7 une clef k_{13} de la même façon que les clefs d'indice impair k_{2i-1} sont ajoutées dans le tour i : $c^{(1)} = x_7^{(1)} \oplus k_{13}^{(1)}, c^{(2)} = x_7^{(2)} \boxplus k_{13}^{(2)}, \dots$.

(a) Du point de vue de la sécurité, quel est le but des fonctions S ? Quel est celui des trois rangées de fonctions L ?

(b) Montrer que $z_i^{(3)} + z_i^{(4)} \equiv x_{i+1}^{(3)} + x_{i+1}^{(4)} \pmod 2$, pour $1 \leqslant i \leqslant 6$.

On suppose dans les deux questions suivantes que $\Pr_{a \in \mathrm{I}}[a \equiv \mathrm{S}(a) \pmod 2] = \frac{1}{2} + \epsilon$, avec $0 < \epsilon < \frac{1}{2}$.

(c) En considérant les clefs de tours fixées, et en faisant varier $x_i^{(3)}$ et $x_i^{(4)}$, quelle est la probabilité que $x_i^{(3)} + x_i^{(4)} \equiv z_i^{(3)} + z_i^{(4)} \pmod 2$, pour $1 \leqslant i \leqslant 6$?

(d) En considérant toujours les clefs de tours fixées, quelle est la probabilité que lors d'un chiffrement, $u_1^{(3)} + u_1^{(4)} \equiv c^{(3)} + c^{(4)} \pmod 2$. En déduire une attaque à clairs connus sur ce chiffrement.

(e) On définit la fonction S comme la fonction $\mathrm{S} : \mathrm{I} \to \mathrm{I},\ a \mapsto (45^a \mod 257) \mod 256$. On admet que S est bien une permutation de l'ensemble I. Montrer que $\mathrm{S}(a + 128) \equiv \mathrm{S}(a) + 1 \pmod 2$, pour tout $a \in \mathrm{I}$. L'attaque est elle possible avec ce choix pour S?

$\boxed{4}$ Construction de fonctions 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. 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.

(a) 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 $n = k$

(b) Ces fonctions sont elles résistantes aux collisions?

(c) 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, $\overline{x} = x \oplus (11 \ldots 1)$, 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.