Master CSI 2 2019-2020

Cryptanalyse — 4TCY902U

Responsable : G. Castagnos

Examen — mardi 17 décembre 2019

Durée 3h
Documents non autorisés
Les exercices sont indépendants

1 Attaque sur un LFSR filtré

On considère un chiffrement à flot de type LFSR filtré. Ce chiffrement à flot utilise un unique LFSR de longueur 128 avec un polynôme de rétroaction public primitif. Au temps $t = 0$, une clef secrète de 128 bits est chargée dans le registre du LFSR. On note $S^{(t)} = (S_0^{(t)}, S_1^{(t)}, \dots, S_{127}^{(t)})$ l'état interne au temps t. Pour tout $t \geqslant 0$, le bit de suite chiffrante z_t au temps t est obtenu en appliquant une fonction de filtrage f sur l'état interne au temps t :

$$z_t := f(S_0^{(t)}, S_1^{(t)}, \dots, S_{127}^{(t)}) := S_{127}^{(t)} + \sum_{i=0}^{62} S_i^{(t)} S_{\alpha(i)}^{(t)} + S_{10}^{(t)} S_{23}^{(t)} S_{32}^{(t)} S_{42}^{(t)} + \prod_{i=0}^{62} S_i^{(t)} +$$

$$+ S_1^{(t)} S_2^{(t)} S_9^{(t)} S_{12}^{(t)} S_{18}^{(t)} S_{20}^{(t)} S_{23}^{(t)} S_{25}^{(t)} S_{26}^{(t)} S_{28}^{(t)} S_{33}^{(t)} S_{38}^{(t)} S_{41}^{(t)} S_{42}^{(t)} S_{51}^{(t)} S_{53}^{(t)} S_{59}^{(t)},$$

où α est une bijection de $\{0, \dots, 62\}$ dans $\{63, \dots, 125\}$. Puis le registre du LFSR est mis à jour de manière usuelle : $S_i^{(t+1)} = S_{i+1}^{(t)}$, pour $0 \leqslant i \leqslant 126$, et $S_{127}^{(t+1)}$ est mis à jour par une combinaison linéaire dans $\mathbf{F}_2$ de $S_0^{(t)}, S_1^{(t)}, \dots, S_{127}^{(t)}$, en fonction du polynôme de rétroaction.

(a) Expliquer comment Alice et Bob peuvent utiliser ce générateur afin d'échanger N bits de manière confidentielle.

(b) Dans cette question, on suppose qu'un attaquant connaît le bit de suite chiffrante au temps t, z_t. Montrer que s'il connaît de plus 63 bits de l'état interne au temps t (préciser lesquels), alors il peut écrire une équation linéaire dont les inconnues sont les autres bits du registre au temps t.

(c) Déduire de la question précédente une attaque permettant de retrouver la clef secrète, en supposant connu de l'attaquant les 33 premiers bits de suite chiffrante. Quelle est la complexité de cette attaque ?

(d) Que vaut $f(S_0^{(t)}, S_1^{(t)}, \dots, S_{127}^{(t)})(1 + S_{23}^{(t)})$? Montrer que l'on peut obtenir une expression similaire en multipliant f par $(1 + S_i^{(t)})$ pour un certain entier i (à préciser) avec $i \neq 23$ et $0 \leqslant i \leqslant 127$.

(e) En déduire une attaque plus performante que la précédente contre ce chiffrement à flot visant à retrouver la clef secrète. Donner la complexité de cette attaque et le nombre de bits de suite chiffrante nécessaires pour la mettre en œuvre.

2 Le chiffrement à flot SG

On considère un chiffrement à flot synchrone additif noté SG dans la suite. Ce système utilise deux LFSR : $\mathrm{LFSR_A}$ et $\mathrm{LFSR_S}$ de longueurs respectives ℓ_A et ℓ_S. Les états initiaux des deux LFSR notés K_A et K_S constituent la clef secrète. Les rétroactions de ces deux LFSR sont publiques, on choisit comme polynômes de rétroaction des polynômes primitifs. La production de la suite de bits chiffrante se fait ainsi :

On répète les trois points suivants jusqu'à produire assez de suite chiffrante :

1. Les $\mathrm{LFSR_A}$ et $\mathrm{LFSR_S}$ sont mis à jour, produisant deux bits a et s ;
2. Si le bit de sortie s du $\mathrm{LFSR_S}$ vaut 0 alors on ne fait rien ;
3. Sinon si $s = 1$, alors le bit de sortie de SG est le bit de sortie du $\mathrm{LFSR_A}$, a.

Par exemple, le $\mathrm{LFSR_A}$, de longueur $\ell_A = 3$, de polynôme de rétroaction $P_A = 1 + X + X^3$ initialisé par $K_A = [1,0,1]$ produit la suite de période $1,0,1,0,0,1,1$. Le $\mathrm{LFSR_S}$ de longueur $\ell_S = 2$ de polynôme de rétroaction $P_S = 1 + X + X^2$ initialisé par $K_S = [0,1]$ produit la suite de période $0,1,1$. Avec ces choix, la suite produite par SG est $0,1,0,1,1,0,0,0,\ldots$

Dans la suite on notera $(a_t)_{t\in\mathbf{N}}$, $(s_t)_{t\in\mathbf{N}}$ et $(z_t)_{t\in\mathbf{N}}$ les suites de sorties respectives du $\mathrm{LFSR_A}$, du $\mathrm{LFSR_S}$ et de SG. Soit $i \in \mathbf{N}$, on note k_i la position du $(i+1)$-ième « 1 » dans la suite $(s_t)_{t\in\mathbf{N}}$. Ainsi, on a $z_i = a_{k_i}$.

(a) On note T_A et T_S les périodes respectives des suites $(a_t)_{t\in\mathbf{N}}$ et $(s_t)_{t\in\mathbf{N}}$. Que valent, d'après le cours, T_A et T_S en fonction de ℓ_A et ℓ_S ?

(b) On note W_S le nombre de 1 dans une période de la suite produite par le $\mathrm{LFSR_S}$. Que vaut W_S en fonction de ℓ_S ? Démontrer ce résultat.

(c) Montrer que pour $i, j \in \mathbf{N}$, $z_{i+jW_S} = a_{k_i+jT_S}$. En déduire que la période de la suite $(z_t)_{t\in\mathbf{N}}$ divise $T_A W_S$.

(d) On suppose que $\mathrm{pgcd}(T_A, T_S) = 1$. On admet que pour tout $k \in \mathbf{N}$, la suite $(a_{k+jT_S})_{j\in\mathbf{N}}$ est une m-suite produite par un LFSR de longueur ℓ_A. En déduire un polynôme de rétroaction pour la suite $(z_t)_{t\in\mathbf{N}}$ et une majoration de sa complexité linéaire.

(e) Question indépendante des questions précédentes. On suppose que l'on a accès aux bits de sortie de SG. 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 ?

3 Attaque sur un système à clef publique

On considère le chiffrement à clef publique suivant. Pour construire ses clefs, Bob choisit un grand entier $q > 0$, et deux entiers f et g tels que $f < \sqrt{q/2}$, $\sqrt{q/4} < g < \sqrt{q/2}$ et $\text{pgcd}(f,q) = \text{pgcd}(f,g) = 1$. Il calcule ensuite $h \equiv f^{-1}g \pmod{q}$ avec $0 < h < q$. Sa clef publique est (h,q) et sa clef privée est (f,g).

Pour envoyer à Bob un message clair m, un entier avec $0 < m < \sqrt{q/4}$, Alice choisit un entier r aléatoire avec $0 < r < \sqrt{q/2}$ et calcule le chiffré $c \equiv m + rh \pmod{q}$.

(a) Pour déchiffrer c avec sa clef privée (f,g), Bob commence par calculer $A \equiv fc \pmod{q}$. Donner la suite de l'algorithme de déchiffrement et montrer qu'il retourne un résultat correct.

(b) Montrer de manière informelle comment utiliser le réseau $\mathscr{L}$ de $\mathbf{R}^2$ de base

$$\begin{pmatrix} 1 & h \\ 0 & q \end{pmatrix}$$

pour définir un algorithme polynomial en la taille de q qui retrouve la clef privée à partir de la clef publique.

4 Attaques sur un chiffrement par bloc

(a) Question préliminaire : Soit F un chiffrement par blocs opérant sur des blocs de n bits avec une clef secrète de k bits. On suppose connu un couple clair chiffré (X, Y) tel que $Y = F_K(X)$ pour une clef secrète K fixée. On suppose que $F_{K^\star}(X)$ est uniformément distribué quand on fait varier des clefs $K^\star$. Montrer qu'à l'issu d'une recherche exhaustive recherchant K à partir de (X, Y), on peut s'attendre à avoir 2^{k-n} candidats pour cette clef K.

On note $\text{DES}_K(X)$ la fonction de chiffrement du DES, qui prend en entrée un bloc de message X de 64 bits, une clef K de 56 bits et ressort un bloc de 64 bits. On construit un nouveau chiffrement par bloc en faisant 6 tours de schéma de Feistel avec 6 clefs de 56 bits indépendantes notées $K_1, K_2, \ldots, K_6$, en utilisant la fonction DES comme fonction de tour. Plus précisément, soit M un bloc de 128 bits à chiffrer. On pose $M = L_0 \| R_0$ avec L_0 et R_0 de 64 bits, puis pour $i \in \{1, \ldots, 6\}$,

$$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus \text{DES}_{K_i}(R_{i-1})$$

Le chiffré est $C = R_6 \| L_6$.

(b) On suppose connu un couple clair chiffré (M, C) par ce nouveau schéma de chiffrement. Donner une attaque utilisant $2^{169} = 2^{3\times 56+1}$ chiffrements DES visant à retrouver les clefs $K_1, \ldots, K_6$. À l'issue de votre attaque combien reste-t-il en moyenne de candidats possibles pour ces clefs (en faisant toujours l'hypothèse habituelle que les sorties des tours sont indépendantes et uniformément distribuées quand on fait varier les clefs)? Combien faudrait il de couples clairs chiffrés pour n'avoir plus qu'un candidat en moyenne? Décrire cette attaque utilisant plusieurs couples clairs chiffrés.

(c) Soit $\Delta \neq 0$ un bloc de 64 bits non nul. On considère deux messages clairs $M = L_0 \| R_0$ et $M^\star = L_0^\star \| R_0^\star$ tel que $L_0 \oplus L_0^\star = \Delta$ et $R_0 = R_0^\star$. On note $L_5 \| R_5$ (resp. $L_5^\star \| R_5^\star$) l'entrée du dernier tour lors du chiffrement de M (resp. de $M^\star$). Montrer qu'il est impossible d'avoir simultanément $L_5 = L_5^\star$ **et** $R_5 \oplus R_5^\star = \Delta$.

(d) Soit X un bloc fixé de 64 bits. On considère N messages clairs de la forme $M^{(i)} = L_0^{(i)} \| X$ pour $i = 1, \ldots, N$ où $L_0^{(i)}$ est choisi au hasard de manière uniforme parmi les blocs de 64 bits. On note $C^{(i)} = R_6^{(i)} \| L_6^{(i)}$ le chiffré de $M^{(i)}$ pour $i = 1, \ldots, N$. En supposant les $C^{(i)}$ uniformément distribués et indépendant des messages clairs, combien y aura-t-il en moyenne de paires d'éléments distincts i, j tels que $L_6^{(i)} \oplus L_6^{(j)} = L_0^{(i)} \oplus L_0^{(j)}$?

(e) Déduire des deux questions précédentes une attaque à messages clairs choisis visant à retrouver la clef K_6 de dernier tour. Combien de messages clairs choisis et combien de chiffrements DES sont nécessaires pour éliminer environ la moitié des clefs possibles pour K_6 ? On pourra utiliser le fait que pour tout réel z, $1 - z \leqslant e^{-z}$ et que $1 - e^{-1} \approx 0,63$.