Exercices et problèmes de cryptographie
Damien Vergnaud
Exercice complémentaire n° 3.20 et 3.21

Les *attaques par décalage* (*slide attacks*, en anglais) ont été introduites par A. BIRYUKOV et D. WAGNER en 1999 à la conférence FSE . Elles s'appliquent aux systèmes de chiffrement itératifs où la fonction de tour est vulnérable à une attaque à deux clairs connus et où la diversification de clé utilisée est relativement simple (par exemple utilisant des sous-clés périodiques). Cette technique est particulièrement adaptée aux systèmes de chiffrement qui utilisent un grand nombre de tours puisque la complexité des attaques l'utilisant est généralement indépendante de ce nombre de tours.

Le système de chiffrement par bloc TREYFER a été proposé par G. YUVAL en 1997 à la conférence FSE. Il s'agit d'un système très efficace qui avait pour but de pouvoir être implanté sur des cartes à puces. Le système TREYFER utilise une clé de 64 bits pour chiffrer des blocs de 64 bits. Il est très compact (*cf.* Figure (1)) et son pseudo-code est donné dans l'algorithme (1) où S est une S-boîte de $(\mathbb{Z}/256\mathbb{Z})$:

Algorithme 1 Système de chiffrement par bloc TREYFER

ENTRÉE: texte, $K \in (\mathbb{Z}_{256})^8$
SORTIE: chiffre $\in (\mathbb{Z}_{256})^8$
  pour r de 0 à 31 **faire**
    texte[8] $\leftarrow$ texte[0] ▷ variable temporaire
    pour i de 0 à 7 **faire**
      texte$[i+1] \leftarrow (\text{texte}[i+1] + S(\text{texte}[i] + K[i]) \bmod 256) \lll 1$
      ▷ (rotation de 1 bit vers la gauche)
    fin pour
    texte[0] $\leftarrow$ texte[8]
  fin pour
  retourner texte[0], texte[1], ..., texte[7]

En particulier, nous voyons que le système TREYFER applique 32 fois la même permutation que nous notons π_K. L'exercice suivant montre qu'une attaque (à textes clairs connus) par décalage utilisant cette propriété permet de retrouver la clé K plus rapidement qu'une recherche exhaustive.

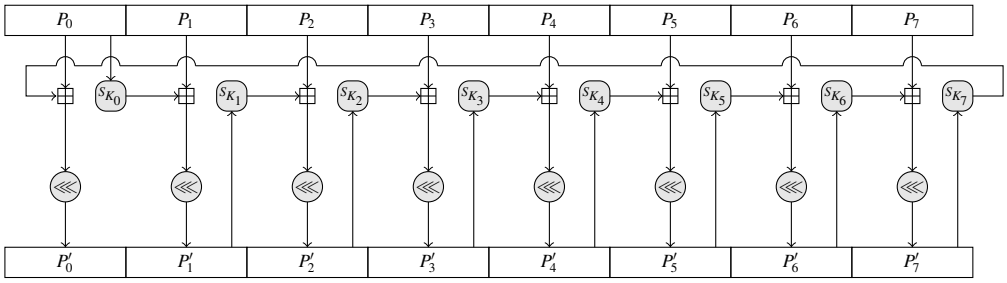

FIGURE 1 – Description du système de chiffrement par bloc TREYFER

Exercice 3.20 ATTAQUE PAR DÉCALAGE SUR TREYFER

1. Soient deux messages clairs M et M^* de $(\mathbb{Z}_{256})^8$ et C et C^* les textes chiffrés correspondants. Montrer que si $\pi_K(M) = M^*$, alors $\pi_K(C) = C^*$.
2. Montrer que si un tel couple de message est connu, alors il est facile de retrouver la clé K utilisée.
3. En déduire une attaque pour retrouver la clé qui utilise 2^{32} textes clairs connus en effectuant l'équivalent de 2^{59} chiffrements TREYFER.
4. En remarquant que si l'adversaire connaît deux octets consécutifs de clés, il peut accélérer le test précédent d'un facteur 2^{32}, proposer une attaque pour retrouver la clé qui utilise 2^{32} clairs connus en effectuant l'équivalent de 2^{44} chiffrements TREYFER.

Solution :

1. Par définition de TREYFER, nous avons $C = \pi_K^{32}(M)$ et $C^* = \pi_K^{32}(M^*)$. Par conséquent, si $\pi_K(M) = M^*$, nous avons
$$\pi_K(C) = \pi_K(\pi_k^{32}(M)) = \pi_K^{32}(\pi_K(M)) = \pi_K^{32}(M^*) = C^*.$$

2. Si $M^* = \pi_K(M)$, il est très facile de retrouver $K = (K_0, \ldots, K_7)$ octet par octet puisque la permutation π n'est appliquée qu'une fois. Par exemple, en notant M_i et M_i^* pour $i \in \{0, \ldots, 7\}$ les octets constituants M et M', nous avons
$$M_{i+1}^* \leftarrow (M_{i+1} + S(M_i^* + K_i) \bmod 256) \lll 1$$
pour $i \in \{1, \ldots, 6\}$ et donc
$$K_i = S^{-1}((M_{i+1}^* \ggg 1) - M_{i+1} \bmod 256) - M_i^* \bmod 256)$$
pour $i \in \{1, \ldots, 6\}$. De même nous trouvons facilement les valeurs de K_0 et K_7.

3. Un attaquant peut simplement appliquer la méthode de la question précédente pour tester la clé K utilisée par la permutation π. Pour chaque paire de clairs et chaque paire de chiffrés associés, il calcule les clés K correspondantes avec la méthode de la question précédente et conserve les paires qui donnent la même valeur K. Il suffit donc d'appliquer la méthode aux $2^{32}(2^{32}-1)/2 \simeq 2^{63}$ couples de clairs et aux 2^{63} couples de chiffrés correspondants jusqu'à obtenir une telle collision de clés. Le coût du calcul de K est égal à $1/32$ du coût de l'évaluation de TREYFER, donc le coût algorithmique de cette étape est égale à $2 \cdot 2^{-5} 2^{63} = 2^{59}$ évaluations de TREYFER. Par le paradoxe des anniversaires, la probabilité de succès de l'attaquant est supérieure à $1/2$ et le nombre de mauvaises clés produites par cette attaque sera relativement faible (et peut être réduit si nécessaire par les techniques classiques de filtrage).

4. Si l'attaquant connaît deux octets consécutifs de la clé K, il obtient une relation entre 16 bits des messages M et M^* et une relation entre 16 bits des chiffrés C et C^* pour que $\pi_K(M) = M^*$ et $\pi_K(C) = C^*$. En utilisant ces relations, il n'a pas besoin de tester tous les 2^{63} couples de clairs et de chiffrés de l'attaque précédente mais peut les filtrer très rapidement et n'avoir (en moyenne) qu'à tester 2^{32} couples. Le coût de l'attaque si l'attaquant connaît deux octets consécutifs est donc réduit à 2^{28} et en faisant une recherche exhaustive sur deux octets de clé, le coût de l'attaque devient égal à $2^8 \cdot 2^8 \cdot 2^{28} = 2^{44}$.

□

La technique de l'exercice précédent s'applique à tous les systèmes de chiffrement itératifs qui utilisent la même permutation à chaque tour (si la fonction de tour est vulnérable à une attaque à deux clairs connus). Nous allons voir qu'elle s'applique également si le système de chiffrement utilise des sous-clés périodiques.

Considérons une variante du système de chiffrement DES obtenue en augmentant la taille de la clé et le nombre de tours de la façon suivante :

- le nombre de tours est augmenté de 16 à 64 ;
- la taille de la clé K est augmentée de 56 à 96 bits et la diversification de clé consiste simplement à utiliser les 48 premiers bits de K dans les tours impairs et les 48 derniers bits de K dans les tours pairs.

Ce système de chiffrement, appelé $2K-DES$, semble plus sûr que le chiffrement DES contre les attaques par force brute (la taille de la clé est significativement augmentée) et contre les attaques par cryptanalyse différentielle ou linéaire (l'augmentation du nombre de tours rendant ces attaques très difficiles).

Exercice 3.21 ATTAQUE PAR DÉCALAGE SUR $2K-DES$

Montrer que le système $2K-DES$ est vulnérable à une attaque par décalage utilisant 2^{48} textes clairs choisis et de complexité équivalente à 2^{43} chiffrements $2K-DES$.

Solution : L'attaque est très proche de l'attaque sur TREYFER décrite dans l'exercice précédent. Il suffit de remarquer que le chiffré C d'un message M est obtenu en appliquant 64 fois la fonction de tour du DES notée F en alternant les deux clés K_1 et K_2 :

$$C = \mathscr{E}_K(M) = F_{K_2}(F_{K_1}(F_{K_2}(F_{K_1}(\ldots F_{K_2}(F_{K_1}(M))\ldots)))) = (F_{K_2} \circ F_{K_1})^{32}(M).$$

Notons F_1 la fonction de tour du DES avec la clé K_1 et mais sans échange des parties droite et gauche et F_2 la fonction de tour du DES avec la clé K_2 mais avec échange des parties droite et gauche avant et après. Nous avons encore :

$$C = \mathscr{E}_K(M) = F_2(F_1(F_2(F_1(\ldots F_2(F_1(M))\ldots)))) = (F_2 \circ F_1)^{32}(M).$$

Posons

$$C' = F_2^{-1}(C) = (F_1 \circ (F_2 \circ F_1)^{31})(M),$$

comme les transformations F_1 et F_2 sont des involutions pour toute clé k (par le choix de la répartition des échanges des parties droite et gauche dans le schéma de Feistel), nous avons

$$\begin{aligned}
\mathscr{E}_K(C') &= [(F_2 \circ F_1)^{32} \circ F_1 \circ (F_2 \circ F_1)^{31}](M) \\
&= [(F_2 \circ F_1)^{31} \circ F_2 \circ (F_2 \circ F_1)^{31}](M) \\
&= [(F_2 \circ F_1)^{31} \circ F_1 \circ (F_2 \circ F_1)^{30}](M) \\
&\vdots \\
&= [F_2 \circ F_1 \circ F_1](M) \\
&= F_2(M)
\end{aligned}$$

qui ne dépend que de la clé K_2 et du message M.

Un attaquant peut donc simplement faire une recherche exhaustive sur la clé K_2 ; pour chaque clé candidate, calculer le déchiffrement partiel $C' = F_{K_2}^{-1}(C)$, demander le chiffrement $\mathscr{E}_K(C')$ de C' et vérifier qu'il est égal à $F_{K_2}(M)$ pour la clé K_2 testée. L'attaque demande autant de clairs choisis que de choix possibles pour K_2 (soit 2^{48}) et nécessite un chiffrement partiel et un déchiffrement partiel d'un tour par clé testée (ce qui correspond à $1/32$-ème du coût du chiffrement complet de $2\mathsf{K}-\mathsf{DES}$). Le coût complet de l'attaque est donc équivalent à $2^{48} \cdot 2^{-5} = 2^{43}$ chiffrements complets $2\mathsf{K}-\mathsf{DES}$. □