Université de Perpignan Année 2012
C. Negre

TD 3 Cryptographie

Attaques sur des chiffrements par bloc

Exercice 1. Soit $S\colon \{0,1\}^\ell \to \{0,1\}^\ell$ un fonction de substitution. Montrer que $N^D_{\Delta\to\Delta^\star}(S)$ est toujours pair.

Exercice 2 (Attaque differentielle)**.** On considère un SPN à quatre ronde décrit dans la figure 1

- La boite S est donnée par

X	$[0,0,0,0]$	$[0,0,0,1]$	$[0,0,1,0]$	$[0,0,1,1]$	$[0,1,0,0]$	$[0,1,0,1]$	$[0,1,1,0]$	$[0,1,1,1]$
$S(X)$	$[1,1,1,0]$	$[0,0,1,0]$	$[0,0,0,1]$	$[0,0,1,1]$	$[1,1,0,1]$	$[1,0,0,1]$	$[0,0,0,0]$	$[0,1,1,0]$
X	$[1,0,0,0]$	$[1,0,0,1]$	$[1,0,1,0]$	$[1,0,1,1]$	$[1,1,0,0]$	$[1,1,0,1]$	$[1,1,1,0]$	$[1,1,1,1]$
$S(X)$	$[1,1,1,1]$	$[0,1,0,0]$	$[0,1,0,1]$	$[1,0,1,0]$	$[1,0,0,0]$	$[1,1,0,0]$	$[0,1,1,1]$	$[1,0,1,1]$

- La permutation P est donnée par

$$P([u_1,\ldots,u_{12}]) = [u_5,u_9,u_2,u_7,u_{10},u_1,u_4,u_{11},u_6,u_3,u_{12},u_8]$$

- Les clefs de ronde $K_0,\ldots,K_3$ sont toutes égale à $K=[k_1,\ldots,k_{12}]$ la clef de chiffrement.

1. Sur la page web suivante

   `http://perso.univ-perp.fr/christophe.negre/Enseignement/Cryptographie/Master1/`

   vous trouverez un code C implémentant le SPN proposé. Ce code s'appuit sur des fonctions `SBoite` implémentant la couche de sustitution d'une ronde, `P` effectuant la permutation des bits et `addkey` faisant le XOR bit à bit avec la clef et une fonction `chiffrement` effectuant les 4 rondes du SPN.

   Vous complèterez le code pour la partie déchiffrement:

   (a) Une fonction `SBoiteinverse` qui effectue la substitution inverse par la fonction réciproque de S, vous utiliserez un tableau pour stoquer la fonction réciproque de S.

   (b) Une fonction `Pinverse` qui effectue la permutation inverse des bits. Vous utiliserez pour cela les operateurs `^` qui effectue un XOR bit à bit, `&` qui effectue un AND bit à bit et `>>` et `<<` qui effectuent des decalages à droite et à gauche.

   (c) Une fonction `dechiffrement` qui effectue le de chiffrement d'un bloc.

2. Calculer les valeurs de $N^D_{\Delta\to\Delta^\star}$ de S pour

$$(\Delta,\Delta^\star) = ([1,0,0,1],[0,0,0,1]),$$
$$(\Delta,\Delta^\star) = ([0,0,1,0],[1,1,1,1]),$$

   Vous pouvez utiliser le programme C pour effectuer ce calcul.

3. Trouver une propagation de différence pour les 3 premières rondes du SPN en commençant par une relation sur la boite de gauche et en prenant pour les autres boites la propagation triviale $0\to 0$.

4. En utilisant le code C de la question 1, chiffrer une série de couple de message clair vérifiant la différence trouvée dans la question 2. avec une clef de votre choix. Monter ensuite une attaque differentielle en utilisant la relation trouvée dans la question précédente.

Exercice 3 (Attaque par saturation sur AES).

- *Étape 1.* Nous considérons une attaque à messages clairs choisis contre une variante de l'AES réduite à 4,5 et 6 tours. L'attaquant demande le chiffrement de 256 clairs $M_0, M_1, \ldots, M_{255}$ où quinze octets prennent une valeur constante ($\mathfrak{c}$), et un octet (en haut à gauche) prend les 255 valeurs possibles ($\mathfrak{a}$):

$\mathfrak{a}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$

Nous noterons par la suite $C_i^{(j)}$ le chiffré de M_j après j rondes.

1. Montrer que
$$\bigoplus_{u\in\{0,1\}^8} u = 0.$$
2. Montrer qu'après la permière ronde les $C_i^{(1)}$ sont de la forme suivante:

$\mathfrak{a}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{a}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{a}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$
$\mathfrak{a}$	$\mathfrak{c}$	$\mathfrak{c}$	$\mathfrak{c}$

où $\mathfrak{a}$ signifique l'octet prend toutes les valeurs lorque i de $C_i^{(1)}$ varie. En déduire la valeur de $\oplus_{i=0}^{255} C_i^{(1)}$
3. Montrer qu'après la 2eme ronde les $C_i^{(2)}$ sont de la forme suivante:

$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$
$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$
$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$
$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$	$\mathfrak{a}$

En déduire la valeur de $\oplus_{i=0}^{255} C_i^{(2)}$.
4. Maintenant considérer les blocs chiffrer après le SubByte de la 3-ème ronde, dire de quelle forme sont les blocs de messages. En déduire la valeur de $\oplus_{i=0}^{255} C_i^{(3)}$?

- *Étape 2.* Établir un scénario pour les deux cas suivants, basé sur les résultat de la première ronde:
1. Attaque d'AES à 4 rondes : on attaque séparément chacun des octets de la 4-ème ronde.
2. Attaque d'AES à 5 rondes : on attaque 4 octets de la clef de la 5-ème ronde et 1 octets de la 4-ème ronde.
3. En utilisant le code d'AES situé sur la page web

   `http://perso.univ-perp.fr/christophe.negre/Enseignements/Master1`

   vous monterez les attaques à 4 et 5 rondes décrites ci-dessus (Attention: l'attaque sur 5 rondes est gourmande en temps de calcul).

Figure 1: SPN - Attaque diff