Cryptanalyse différentielle et linéaire

Pierre-Alain Fouque

Réseau SP

- Schéma de chiffrement par bloc de taille nm
- Réseau de Substitution-Permutation (SPN)
- Soit n et m deux entiers
- Longueur du clair et chiffré: nm
- Deux composants π_S et π_P:
  - $\pi_S: \{0,1\}^n \rightarrow \{0,1\}^n$ une substitution (S-box)
  - $\pi_P: [1,nm] \rightarrow [1,nm]$ une permutation

Notations

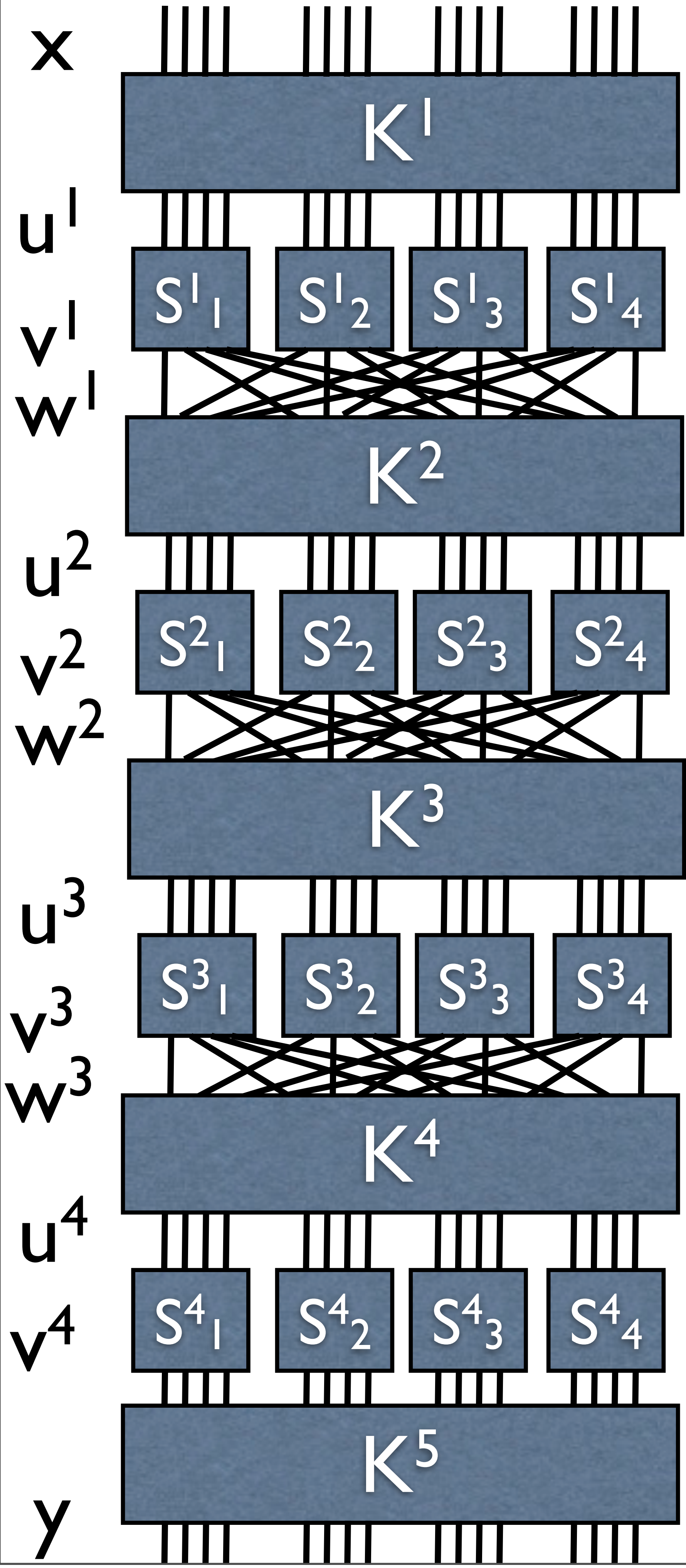
- $x=(x_1,\ldots,x_{nm})=x_{(1)}||\ldots||x_{(m)}\in\{0,1\}^{nm}$, avec $x_{(i)}\in\{0,1\}^n$
- $(K^1,\ldots,K^{e+1})$ les $(e+1)$ sous-clés
- u^k l'entrée des Sbox à l'étage k
- v^k la sortie des Sbox à l'étage k=entrée permutation
- w^k la sortie de la permutation à l'étage k
- S^k_i: i-ième Sbox de l'étage k

z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi_S(z)$	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

z	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\pi_P(z)$	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

Diversification de clé

- Décalage des bits: Pas bonne méthode, mais exemple
- $K = 0011\ 1010\ 1001\ 0100\ 1101\ 0110\ 0011\ 1111 \in \{0,1\}^{32}$,
- $K^1 = 0011\ 1010\ 1001\ 0100$
- $K^2 = 1010\ 1001\ 0100\ 1101$
- $K^3 = 1001\ 0100\ 1101\ 0110$
- $K^4 = 0100\ 1101\ 0110\ 0011$
- $K^5 = 1101\ 0110\ 0011\ 1111$



SPN

- Cryptanalyse linéaire:
  - Supposons qu'on trouve une relation linéaire probabiliste entre un ensemble de bits du texte clair x et un sous-ensemble des bits de l'état v4 (il existe des variables dont le ⊕ vaut 0 avec probabilité ≠ 1/2)
  - Si on a suffisamment de messages chiffrés avec une clé K, alors on peut retrouver la clé K
  - Pour chaque chiffré, on déchiffre le dernier étage et on vérifie la relation avec des compteurs

Lemme d'empilement

- X_1 et X_2 deux variables aléatoires sur $\{0,1\}$
- $Pr[X_i=0]=p_i$ et $Pr[X_i=1]=1-p_i$, $i=1,2$
- $i\neq j$, X_i et X_j indépendants,
  - $Pr[X_i=0, X_j=0]=p_ip_j$
  - $Pr[X_i=0, X_j=1]=p_i(1-p_j)$
  - $Pr[X_i=1, X_j=0]=(1-p_i)p_j$
  - $Pr[X_i=0, X_j=0]=(1-p_i)(1-p_j)$
  - $Pr[X_i\oplus X_j=0]=p_ip_j+(1-p_i)(1-p_j)$
  - $Pr[X_i\oplus X_j=1]=p_i(1-p_j)+(1-p_i)p_j$

Biais et lemme (suite)

- Biais de X_i: $\varepsilon_i = p_i - 1/2$, $-1/2 \leq \varepsilon_i \leq 1/2$
- $Pr[Xi=0]=1/2+\varepsilon_i$ et $Pr[Xi=1]=1/2-\varepsilon_i$
- Soit i1,...,ik k v.a. Quel est le biais de $X_{i1} \oplus ... X_{ik}$ $\varepsilon_{i1,..,ik}$ en fonction des ε_i ?
- Lemme: $\varepsilon_{i1,..,ik} = 2^{k-1} \prod_{j=1}^{k} \varepsilon_{ij}$ (par récurrence)
- Corollaire: Si $\varepsilon_{ij}=0$ pour un des j, $\varepsilon_{i1,..,ik}=0$ (One-Time-Pad)
- Attention: Résultat pas vrai si pas indépendant: $\varepsilon_1=\varepsilon_2=\varepsilon_3=1/4$, $\varepsilon_{1,2}=\varepsilon_{2,3}=\varepsilon_{1,3}=1/8$, alors que $2\varepsilon_{1,2}\times\varepsilon_{2,3}=1/32$

Approximation Sbox

- Sbox n bits vers n bits
- n variables aléatoires en entrée X_i
- $Pr[X_1=x_1,...X_n=x_n]=1/2^n$
- $y=(y_1,...,y_n)$ les n bits de sorties
- $Pr[X_1=x_1,...,X_n=x_n,Y_1=y_1,...,Y_n=y_n]=0$ si $y\neq\pi_S(x)$ et 2^{-n} sinon.
- Quel est le biais de $X_{i1}\oplus...\oplus X_{ik}\oplus Y_{j1}\oplus...\oplus Y_{jl}$?

Exemple Sbox

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

Soit $X_1 \oplus X_4 \oplus Y_2$

$\Pr[X_1 \oplus X_4 \oplus Y_2 = 0]$
$= 1/2$

$\Pr[X_1 \oplus X_4 \oplus Y_2 = 1]$
$= 1/2$

Biais de
$X_3 \oplus X_4 \oplus Y_1 \oplus Y_4$:
-3/8

Représentation résultat

- $2^8=256$ biais à évaluer de la forme $(\oplus_{i=1}^{4} a_i X_i) \oplus (\oplus_{i=1}^{4} b_i Y_i)$ avec $a_i \in \{0,1\}$ et $b_i \in \{0,1\}$ pour $i=1,\ldots,4$ qu'on représente de façon compacte (a_1,a_2,a_3,a_4) et (b_1,b_2,b_3,b_4) en hexa
  - Ex: $X_1 \oplus X_4 \oplus Y_2$ entrée $(1,0,0,1)=9$ hexa et sortie $(0,1,0,0)=4$ en hexa
- Pour chacune, on compte le nombre de ligne qui satisfait la relation $\varepsilon(a,b)=(N_L(a,b)-8)/16$
  - Ex: $N_L(9,4)=8$, $\varepsilon(9,4)=0$
  - cf. Table d'approximation linéaire

Cryptanalyse linéaire SPN

- Les Sbox qui ont une entrée avec une flèche entrante sont appelées actives
- dans S^1_2, v.a. $T_1=U^1_5 \oplus U^1_7 \oplus U^1_8 \oplus V^1_6$: biais=1/4
  dans S^2_2, v.a. $T_2=U^2_6 \oplus V^2_6 \oplus V^2_8$: biais=-1/4,
- dans S^3_2, v.a. $T_3=U^3_6 \oplus V^3_6 \oplus V^3_8$: biais=-1/4
- dans S^3_4, v.a. $T_4=U^3_{14} \oplus V^3_{14} \oplus V^3_{16}$: biais=-1/4
- T_1,T_2,T_3,T_4 ont un biais important en valeur absolue

Un peu de calcul ...

- Supposons que ces variables aléatoires soient indépendantes ...
- le lemme d'empilement dit que le biais de $T_1 \oplus T_2 \oplus T_3 \oplus T_4$ est $2^3(1/4)(-1/4)^3=-1/32$
- On remarque que $T_1 \oplus T_2 \oplus T_3 \oplus T_4$ s'exprime en fonction de x, u^4 et de bits de clés
- $T_1=U^1{}_5 \oplus U^1{}_7 \oplus U^1{}_8 \oplus V^1{}_6=X_5 \oplus K^1{}_5 \oplus X_7 \oplus K^1{}_7 \oplus X_8 \oplus K^1{}_8 \oplus V^1{}_6$
- $T_2=U^2{}_6 \oplus V^2{}_6 \oplus V^2{}_8=V^1{}_6 \oplus K^2{}_6 \oplus V^2{}_6 \oplus V^2{}_8$
- $T_3=U^3{}_6 \oplus V^3{}_6 \oplus V^3{}_8=V^2{}_6 \oplus K^3{}_6 \oplus V^3{}_6 \oplus V^3{}_8$, ...

suite des calculs

- $X_5 \oplus X_7 \oplus X_8 \oplus V^3{}_6 \oplus V^3{}_8 \oplus V^3{}_{14} \oplus V^3{}_{16} \oplus K^1{}_5 \oplus K^1{}_7 \oplus K^1{}_8 \oplus K^2{}_6 \oplus K^3{}_6 \oplus K^3{}_{14}$ a un biais de -1/32
- On remplace $V^3{}_i$ par $U^4{}_i$ et $V^3{}_6 = U^4{}_6 \oplus K^4{}_6$, $V^3{}_8 = U^4{}_{14} \oplus K^4{}_{14}$, $V^3{}_{14} = U^4{}_8 \oplus K^4{}_8$, $V^3{}_{16} = U^4{}_{16} \oplus K^4{}_{16}$
- Comme les bits de clés ont une valeur fixe pour tous les messages, la variable aléatoire $X_5 \oplus X_7 \oplus X^8 \oplus U^4{}_6 \oplus U^4{}_8 \oplus U^4{}_{14} \oplus U^4{}_{16}$ a un biais de -1/32

Algorithme

- Si on devine les 8 bits de la dernière sous-clé correctement, alors on pourra calculer le biais de la variable aléatoire
- Si on n'a pas la bonne valeur de clé, la variable aléatoire aura un biais proche de 0
- En utilisant des compteurs, on trouvera le biais (maximal) et on déduira qu'on a alors la bonne valeur pour ces 8 bits de clé
- On retrouvera les autres avec une recherche exhaustive

Un peu de statistique...

- Si on a un biais de ε, alors il faudra c/ε^2 messages pour le détecter avec c une petite constante
- Dans notre cas, si on prend $T=8000$ messages, on aura $c \approx 8$ car $1/\varepsilon^2=1024$
- Comment faire mieux avec moins de messages ...

Cryptanalyse différentielle

- C'est une attaque à messages choisis
- Si on a des messages qui satisfont une $x'=x\oplus x^*$ différence fixée en entrée, au bout d'un certain nombre de tours, la différence de sorties $y'=y\oplus y^*$ vaudra une valeur fixe avec bonne probabilité
- Notation: $\Delta(x')=\{(x,x\oplus x'): x\in\{0,1\}^m\}$
- $\Delta(1011)=\{(0000,1011), (0001,1010),...,(1111,0100)\}$
- Pour chaque valeur de $\Delta(1011)$, on peut calculer les différences de sorties

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2

Cryptanalyse différentielle

- On notera $N_D(x',y')=\#\{(x,x^*)\in\Delta(x'):\pi_S(x)\oplus\pi_S(x^*)=y'\}$
- et avec des notations adaptées comme pour la cryptanalyse linéaire, on calcule la table des différences $N_D(a',b')$ avec a',b' en hexa
- L'addition de clé ne pose pas de problème
- Rapport de propagation $R_P(a',b')=N_D(a',b')/2m$
- $R_P(a',b')=\Pr[\text{xor de sortie}=b'|\text{xor entrée}=a']$

Piste différentielle

- dans S^1_2, Rp(1011,0010)=1/2
- dans S^2_3, Rp(0100,0110)=3/8
- dans S^3_2, Rp(0010,0101)=3/8
- dans S^3_3, Rp(0010,0101)=3/8
- Rp(0000 1011 0000 0000,0000 0101 0101 0000) $=1/2*(3/8)^3 = 27/1024$
- x'= 0000 1011 0000 0000, donne $(v^3)'$= 0000 0101 0101 0000 avec probabilité 27/1024
- et $(u^4)'$=0000 0110 0000 0110

Opération de filtrage

- L'algorithme est similaire à celui pour la cryptanalyse linéaire (on a des compteurs qui vont déterminer 8 bits de la dernière sous-clés) et on augmente les compteurs si la caractéristique différentielle est satisfaite
- En plus, on ne conserve dans le calcul que les «bonnes paires», celles où on n'a pas de différences sur $(u_{(1)}^4)'$ et $(u_{(3)}^4)'$
- $T \approx c/\varepsilon$, avec c une petite constante et T entre 50 et 100 permet de retrouver la clé car $1/\varepsilon \approx 38$.

Conclusion: Construction AES

- AES a été construit en connaissant ces attaques
- Les concepteurs ont montré qu'il n'y avait pas d'attaque car les pistes différentielles ont une probabilité de l'ordre de 2^{-128} au bout de 5 tours
- Les marges de sécurité font que dans certains cas, on peut remonter plusieurs étages ....