Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

10. Exercise sheet
Hand in solutions until Monday, 19 January 2015, 13:59

Exercise 10.1 (Linear cryptanalysis). (14 points)

Suppose that the S-box of the example in the lecture is replaced by the S-box defined by the following substitution:

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

(i) Compute the correlation table for this S-box. [3]

(ii) Find a linear approximation using three active S-boxes, and use the piling-up lemma to estimate the correlation c of the random variable $X_{16} \oplus U_1^4 \oplus U_9^4$. [3]

(iii) Run the attack! Use a fixed key and $\frac{8}{c^2}$ plaintext/ciphertext pairs. [8]

Exercise 10.2 (Linear cryptanalysis of DES). (0+9 points)

Consider the following linear characteristics from Matsui's article on linear cryptanalysis of DES:

$$\begin{aligned}
A:&\quad X[15] \oplus F(X,K)[7,18,24,29] = K[22] && p = \tfrac{12}{64},\\
B:&\quad X[27,28,30,31] \oplus F(X,K)[15] = K[42,43,45,46] && p = \tfrac{22}{64},\\
C:&\quad X[29] \oplus F(X,K)[15] = K[44] && p = \tfrac{30}{64},\\
D:&\quad X[15] \oplus F(X,K)[7,18,24] = K[22] && p = \tfrac{42}{64},\\
E:&\quad X[12,16] \oplus F(X,K)[7,18,24] = K[19,23] && p = \tfrac{16}{64}.
\end{aligned}$$

(i) For each of the given probabilities, compute the correlation as defined in the lecture. [+2]

Consider the fifteen round linear characteristic

E-DCA-ACD-DCA-A

(ii) Show that the given characteristic indeed works for 15 round DES, i.e. show that from it one obtains the linear relation +5

$$\begin{aligned} &P_H[7,18,24] \oplus P_L[12,16] \oplus C_H[7,18,24,29] \oplus C_L[15] \\ &= K_1[19,23] \oplus L_3 \oplus L_7 \oplus L_{11} \oplus K_{15}[22], \end{aligned}$$

where $L_i = K_i[22] \oplus K_{i+1}[44] \oplus K_{i+2}[22]$.

(iii) Show Matsui's claim that this characteristic has correlation $1.19 \cdot 2^{-21}$. +2