Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

4. Exercise sheet
Hand in solutions until Monday, 28 November 2011, 23:59:59h.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 4.1. (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
$S(z)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

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

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

(iii) Run the attack! Use a fixed key and 10000 plaintext/ciphertext pairs. [8]

Exercise 4.2 (Boolean function and the FFT). (15 points)

Consider a boolean function F mapping k bit to a single bit. In the lecture we have shown that the discrete Fourier transform of the function $f\colon \{0,1\}^k \to \{-1,1\},\ x \mapsto (-1)^{f(x)}$ is given by

$$S_f\colon \begin{array}{ccc} \{0,1\}^k & \longrightarrow & \mathbb{C}, \\ \alpha & \longmapsto & \displaystyle\sum_{x\in\{0,1\}^k} (-1)^{\langle \alpha | x\rangle} f(x) \end{array}$$

(i) Give an explicit formula for $S_f(\alpha)$ in the case $k = 1$. [1]

(ii) Implement the Fast Fourier transform as presented in the lecture. Verify its correctness using the explicit formula. [8]

(iii) Use your implementation to compute for each DES S-box the linear table. Hint: Do your computation column-wise. [4]

(iv) For each of the eight DES S-boxes, compute the bias of the random variable $X_2 \oplus Y_1 \oplus Y_2 \oplus Y_3 \oplus Y_4$. [2]

Exercise 4.3 (Linear cryptanalysis of DES). (9 points)

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

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

2 (i) For each of the given probabilities, compute the bias as defined in the lecture.

Consider the fifteen round linear characteristic

E-DCA-ACD-DCA-A

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

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

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

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