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:

<table>
<thead>
<tr>
<th>$z$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S(z)$</td>
<td>4</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>D</td>
<td>6</td>
<td>3</td>
<td>A</td>
<td>C</td>
<td>5</td>
<td>E</td>
<td>7</td>
<td>F</td>
<td>B</td>
<td>9</td>
<td>0</td>
</tr>
</tbody>
</table>

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

(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 $X_{16} \oplus U^4_1 \oplus U^4_9$.

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

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{align*}
A: & \quad X[15] \oplus F(X, K)[7, 18, 24, 29] = K[22] & p = \frac{12}{64}, \\
B: & \quad X[27, 28, 30, 31] \oplus F(X, K)[15] = K[42, 43, 45, 46] & p = \frac{22}{64}, \\
C: & \quad X[29] \oplus F(X, K)[15] = K[44] & p = \frac{32}{64}, \\
D: & \quad X[15] \oplus F(X, K)[7, 18, 24] = K[22] & p = \frac{16}{64}, \\
E: & \quad X[12, 16] \oplus F(X, K)[7, 18, 24] = K[19, 23] & p = \frac{16}{64}.
\end{align*}

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

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

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

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 \( 1.19 \cdot 2^{-21} \).