Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

7. Exercise sheet
Hand in solutions until Monday, 19 December 2011, 23:59:59.

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 7.1 (Differential properties of PRESENT). (8 points)

In the lecture we encountered the theorem that any five round differential characteristic in the cipher PRESENT must contain at least ten active s-boxes. For the proof we denoted by D_j the number of active s-boxes in round j, where $j \in [i-2, i+2]$ for some fixed i. We had shown that we only need to consider the cases where for some j the number of active s-boxes D_j equals one. Your task is to complete the proof. You can take the cases $j \in \{i, i-1, i+1\}$ as granted.

(i) Prove the statement for the case $D_{i-2} = 1$. 4

(ii) Prove the statement for the case $D_{i+2} = 1$. 4

Exercise 7.2 (Two differential characteristics of PRESENT). (7 points)

Consider the two round characteristic

$$0000000000000011$$
$$0000000000030003$$
$$0000000000000011$$

(i) Show that this characteristic has probability 2^{-10}. Which probability do you obtain for 31 round PRESENT when iterating this characteristic? 2

Consider now the five round characteristic

$$0000000000007070$$
$$000000000000000A$$
$$0001000000000000$$
$$0000000010001000$$
$$0000000000880088$$
$$0033000000330033$$

(ii) Compute its probability. How close to the theoretical bound is your result? Why is this characteristic of little practical interest? 5

Exercise 7.3 (Optimizing PRESENT). (7 points)

Consider the following 16-bit permutation P_{16}:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{16}(i)$	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

4 (i) Show that when we define

$$P'(x_3||x_2||x_1||x_0) = P_{16}(x_3)||P_{16}(x_2)||P_{16}(x_1)||P_{16}(x_0),$$

we have $P(P(x)) = P^{-1}(P'(P'(x)))$, where P is the permutation given in the PRESENT specifications.

3 (ii) How does this fact help you to optimize software implementations of PRESENT?

Exercise 7.4 (Implementation details). (20+5 points)

We now will put our hands on a software implementation of PRESENT-80.

10 (i) Implement PRESENT-80 in a programming language of your choice. How many lines of (reasonably formatted) code did you need? The most efficient implementor gets the bonus points.

+5

10 (ii) Experimentally verify the probabilities of Exercise 7.2 using 100000 samples.