Electronic passport and biometrics, winter 2006

MICHAEL NÜSKEN

5. Exercise sheet
Hand in solutions until Tuesday, 5 December, $12^{\underline{15}}$.

Exercise 5.1 (A simple linear attack). (4+4 points)

Each variable in the following stores one byte or eight bits. Consider the function 4

$$f(B, C) = B \oplus C,$$

$K_j = \texttt{0x42}$ for all relevant j, and let (H_1, H_2, H_3) be computed as follows

Algorithm.

Input: A message $(X_0, X_1, X_2, \ldots, X_{n-1})$.
Output: A hash value $H \in \{0,1\}^{3\times 8}$.

1. $(H_1, H_2, H_3) \leftarrow (0, 0, 0)$.
2. For $i = 0..n-1$ do 3–7
3. $\quad (A, B, C) \leftarrow (H_1, H_2, H_3)$.
4. $\quad$ For $j = 0..R-1$ do 5–6
5. $\quad\quad t \leftarrow A \lll 2 + f(B, C) + X_{i+j} + K_j$,
6. $\quad\quad (A, B, C) \leftarrow (t, A, B \lll 1)$.
7. $\quad (H_1, H_2, H_3) \leftarrow (H_1 + A, H_2 + B, H_3 + C)$.
8. Return $H_1|H_2|H_3$.

We consider a message with $n = 1$ and for simplicity we use $R = 1$. Write one of the bits in the output as a function in the input bits in X_0 in the form $f(X_{00}, \ldots, X_{07}) = a_0 X_{00} + \cdots + a_7 X_{07} + a_8$ where $a_i \in \{0, 1\}$ as good as possible. Can you find coefficients a_i such that f and the chosen output bit coincide in, say 75% of all cases?

Try $R = 2$. +4

Exercise 5.2 (Biometrics). (3+2 points)

Consider a chip card that stores your finger prints.

1 (i) Say, the false accept rate is 3%. Where does this induce problems?

1 (ii) Say, the false reject rate is 5%. Where does this induce problems?

1 (iii) Who can benefit from getting this information?

+1 (iv) What kind of protection should be employed?

+1 (v) Do you think people will accept such a card?