Advanced Cryptography: Algorithmic Cryptanalysis

DANIEL LOEBENBERGER, KONSTANTIN ZIEGLER

5. Exercise sheet
Hand in solutions until Saturday, 14 May 2011, 23:59h.

To estimate the average effort you put into solving the following exercises, please add to your solutions the amount of time you spent on the respective questions.

Exercise 5.1 (Fast Walsh transform). (11+8 points)

In the lecture we discussed the Walsh transform of a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined for $M \in \mathbb{F}_2^n$ as

$$(\mathcal{W}f)(M) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle M | x \rangle} (-1)^{f(x)},$$

with the scalar product $\langle M \mid x \rangle = \sum_{i=0}^{n-1} M_i x_i$. Your task is now to develop a fast algorithm for computing the Walsh transform $\mathcal{W}f$ of f.

(i) Specify a trivial algorithm that runs in $\mathcal{O}(2^{2n})$ evaluations of f to compute the Walsh transform. $\boxed{2}$

(ii) Give a simple formula that gives for $n = 1$ the Walsh transform of f. $\boxed{2}$

(iii) Interpret now the vectors x and M as the binary representation of an integer. Prove that for $x < 2^{n-1}$ and $M < 2^{n-1}$ we have $\boxed{2}$

$$(\mathcal{W}f)(M) = (\mathcal{W}f_0)(M) + (\mathcal{W}f_1)(M)$$

where $f_0(x) = f(x)$ and $f_1(x) = f(2^{n-1} + x)$.

(iv) Prove that for $x < 2^{n-1}$ and $M < 2^{n-1}$ we have $\boxed{2}$

$$(\mathcal{W}f)(2^{n-1} + M) = (\mathcal{W}f_0)(M) - (\mathcal{W}f_1)(M)$$

(v) Plug everything together to give a faster algorithm that runs in $\mathcal{O}(n2^n)$ evaluations of f to compute the Walsh transform $\mathcal{W}f$ of f. $\boxed{3}$

(vi) Give an algorithm that realizes the inverse Walsh-transform and prove that it indeed is the inverse of the Walsh-transform algorithm of exercise 5.1 (i). $\boxed{+8}$

Exercise 5.2 (A particular nonlinear function). (4+4 points)

To totally prevent correlation attacks on the filtered generator, a non-linear function $f : \mathbb{F}_2^n \to F_2$ would be needed whose Walsh-transform equals the zero function.

$\boxed{4}$ (i) For $n = 1, 2, 3$ either give such a function or show that it does not exist.

$\boxed{+4}$ (ii) What do you conjecture in general?

Exercise 5.3 (More on LFSRs). (6 points)

Consider a linear function $L_f : \mathbb{F}_2^\ell \to F_2$ and an LFSR on $k \geq \ell$ bits, where L_f takes for each fixed t some bits

$$(x_{t+\delta_0}, x_{t+\delta_1}, x_{t+\delta_2}, \ldots, x_{t+\delta_{\ell-1}})$$

for fixed constants $\delta_0 < \delta_1 < \cdots < \delta_{\ell-1} < k$ and returns

$$y_t = L_f(x_{t+\delta_0}, x_{t+\delta_1}, x_{t+\delta_2}, \ldots, x_{t+\delta_{\ell-1}}).$$

$\boxed{1}$ (i) Show that there is for each $0 \leq i < \ell$ a state $\vec{x}_t^{(i)}$ such that the LFSR in state $\vec{x}_t^{(i)}$ produces as a next bit the bit $x_{t+\delta_i}$.

$\boxed{3}$ (ii) Show that the output of the LFSR in state $\vec{x}_t^{(0)} \oplus \cdots \oplus \vec{x}_t^{(\ell-1)}$ is y_t.

$\boxed{2}$ (iii) Give an argument that in general the sequence $(y_t)_{t\geq 0}$ is the output sequence of the LFSR with initial state $\vec{x}_t^{(0)} \oplus \cdots \oplus \vec{x}_t^{(\ell-1)}$

Exercise 5.4 (Parity checks). (8 points)

Consider the LFSR of $\mathbb{F}_2$ given by the primitive minimal polynomial x^3+x^2+1. It defines a linearly recurrent sequence $(s_n)_{n\geq 0}$ with period $2^3 - 1 = 7$.

$\boxed{1}$ (i) Write down the linear relation defining the output sequence.

$\boxed{3}$ (ii) Assume your register is in state (s_0, s_1, s_2). For $i = 3, \ldots, 9$, give the linear relations defining s_i in terms of s_0, s_1 and s_2.

$\boxed{1}$ (iii) Write down the matrix of coefficients of the relations.

$\boxed{3}$ (iv) Give all systematic equations involving bit s_4 having $d = 3$ terms.