B-it **Stream Ciphers (WS 2008)**

Responsible: Prof. von zur Gathen
Lecturer: L. El Aimani

Tutorial 3: LFSR-based stream ciphers

I The Geffe Generator

The Geffe generator is defined by three maximum-length LFSRs whose lengths L_1, L_2, L_3 are pairwise relatively prime, with nonlinear combining function

$$f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$$

The key stream generated has period $(2^{L_1} - 1).(2^{L_2} - 1).(2^{L_3} - 1)$.

1. Compute the linear complexity of the output sequence.
2. Check the result experimentally.
3. Compute the correlation probability of the output and $x_1(t)$, and $x_3(t)$.
4. Imeplement a function that, given a sufficient segment of the output sequence, recovers the initial state of the first LFSR (Siegenthaler's attack) .

II Trade-off Correlation Immunity/Non Linear Order

Let f be a non linear function of n binary random variables, given in its algebraic normal form:

$$f(x_1, x_2, ..., x_n) = a_0+a_1x_1+a_2x_2+...+a_nx_n+a_{12}x_1x_2+a_{13}x_1x_3+...+a_{12...n}x_1x_2...x_n. \tag{1}$$

1. prove that $a_{1..k} = \sum_{x\in s_{12...k}} f(x)$. Where $s_{12...k} = \{x : x_{k+1} = ... = x_n = 0\}$ for $1 \leq k \leq n-1$ and $s_{12...n} = \{x\}$.
2. Now, in the rest of the exercise, we will consider that f is m_{th} order correlation immune and prove that the presence of certain products in the algebraic form is incompatible with such property. Let $Z = f(x)$ and $N_{12..k} = |\{x : x \in s_{12..k} \text{ and} f(x) = 1\}|$.

- Prove that $P(Z = 1|x_{k+1} = x_{k+2} = ... = x_n) = \frac{N_{12...k}}{2^k}$ and $P(Z = 1) = \frac{N_{12...n}}{2^n}$.
- Use the condition of the correlation immunity to show that $P(Z = 1|x_{k+1} = x_{k+2} = ... = x_n) = P(Z = 1)$.
- Deduce that $N_{12...k} = 2^{k-(n-m)} N_{12...(n-m)}$ for $n - m \leq k \leq n$.
- conclude.
- Explain how to use the above algorithm for any k component $a_{i_1 ... a_{i_k}} = 0$ for $n - m + 1 \leq k \leq n$.