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

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

Tutorial 4: The Summation Generator

I trade-off Correlation Immunity/Linear Complexity

In this exercise, we will show that the trade-off Correlation Immunity/Linear Complexity showed in a previous exercise does no longer exist if the combiner is allowed to have memory.
Let f be a non linear combiner of n binary random variables, m_{th}-order correlation immune. We will define z the random variable $z = f(x_1, ..., x_n)$.

1. Write the definition of f being m_{th}-order correlation immune.
2. Now, and in the rest of the exercise, the combiner f is allowed to have memory. What would be then the definition of correlation immunity of such a combiner.
3. Let's suppose that the output of the combiner resembles a truly random sequence, which means that it is impossible to, given the sequence up to a certain value, guess the next bit. Show that the above equation is equivalent to:
$$I(z_j; x_{i_1}^j, ..., x_{i_m}^j, z^{j-1}) = 0 \tag{1}$$
4. Now the combiner has the form :
$$z_j = \sum_{i=1}^{n} x_{ij} + f'(x_1^{j-1}, ..., x_n^{j-1}) \tag{2}$$
Show that f is $(n-1)^{th}$ order correlation immune.
5. Conclude.

II The Summation Generator: linear complexity

Let a and b two integers expressed in $2-$radix : $a = a_{n-1}2^{n-1} + ... + a_1 2 + a_0$ and $b = b_{n-1}2^{n-1} + ... + b_1 2 + b_0$. Let $z = a + b$ be the real sum (expressed in $2-$radix).

1. Prove that: $z_j = a_j + b_j + c_{j-1}$ where $c_j = a_j b_j + (a_j + b_j)c_{j-1}$. What do you conclude about the non linear order of f.

2. What happens if the adder produces a pair of zeros or ones? is such an event likely to happen when adding periodic sequences?

3. Give an upper bound of the linear complexity of the output.

4. The experience shows that : $LC((z_j)) \leq (2^{L_1} - 1)(2^{L_2} - 1)$ with near equality. Check this result and conclude.

III The Summation Generator: period

Let E be the set of infinite binary periodic sequences. We define the following mapping: $f : E \to \mathbb{Q}$
$(a_i)_{i \in \mathbb{N}} \to \frac{\sum_{i=0}^{T-1} a_i 2^i}{2^T - 1}$ Where T is a multiple of the period.

1. Prove that f is an injective mapping.(first prove that it is a mapping, then that it is injective).

2. Deduce that if $f(a_i)$ is a binary infinite periodic sequence, then there exists $\frac{p}{q} \in \mathbb{Q}$ where $\gcd(p, q) = 1$, moreover, the period is determined by the multiplicative order of 2 modulo q.

3. Let now, (a_i) and (b_i) be two sequences of periods T_1 and T_2. (s_i) denotes the real sum of (a_i) and (b_i) expressed in 2-radix. If $\gcd(T_1, T_2) = 1$ then (s_j) is of period $T_1 T_2$.
   Steps of the proof:

   (3-1) Prove that $f((a_i), (b_i)) = c + \frac{\sum_{i=0}^{T_1 T_2 - 1} s_i 2^i + c}{2^{T_1 T_2} - 1}$ Where c corresponds to the carry to the other period of the sum sequence.$c = 1, c = 0$.

   (3-2) If we consider $f((a_i)) = \frac{p_1}{q_1}$ and $f((b_i)) = \frac{p_2}{q_2}$ where $\gcd(p_i, q_i) = 1$ for $i = 1, 2$ and $a + b = c + \frac{n}{q_1 q_2}$, $c = 0, 1$. Prove that $f((s_i)) = \frac{n}{q_1 q_2}$.

   (3-3) Prove that $\gcd(n, q_1 q_2) = 1$.
   - Prove first that $\gcd((2^{T_1} - 1), (2^{T_2} - 1)) = 1$.
   - Deduce that $\gcd(q_1, q_2) = 1$.
   - Conclude that $\gcd(n, q_1 q_2) = 1$.

   (3-4) Deduce the period of the sum sequence. Conclude.