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

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

Tutorial 2: Linearly Recurrent Sequences

I Linearly Recurrent Sequences

Let $F = \mathbb{Z}_2[x]/f(x)$ be a the **field** of polynomials of degree at most 2 over $\mathbb{Z}_2$. Addition and multiplication of the elements are performed modulothe polynomial $f(x) = x^3 + x + 1$.

1. (1-1) Write down the elements of F?

   (1-2) Calculate the successive powers of the element x in F. What can you conclude?

2. Let $s = (s_n)_{n\in\mathbb{N}} \in \mathbb{Z}_2^{\mathbb{N}}$ be a linearly recurrent sequence over $\mathbb{Z}_2$, so that **operations on the sequence terms are performed in the field $\mathbb{Z}_2$, where addition and multiplication are the "exclusive or" and usual multiplication resp.** , given by the characteristic polynomial $f(x)$ and the initial values $1, 0, 1$ corresponding to s_0, s_1, s_2 resp.

   (2-1) write the linear recurrence satisfied by s.

   (2-2) calculate the values s_3, s_4 and s_5.

   (2-3) check whether the polynomial $x^4 + x^2 + 1$ is a characteristic polynomial of s and justify your claim.

   (2-4) give an upper bound on the least period and justify your answer.

   (2-5) what is the minimal polynomial of s? Justify (you may use the fact that $\mathbb{Z}_2[x]/f(x)$ is a field).

   (2-6) using the fact that the polynomial f is primitive, deduce the least period of the sequence s.

   (2-7) given the six initial values of s, explain how we can mount an attack and generate the rest of the sequence.

   (2-8) describe the LFSR that implements the generation of the sequence s (initial state vector and connection polynomial).

II Computation of the Minimal Polynomial

We consider the linearly recurrent sequence $s = (s)_{i \in \mathbb{N}}$ over $\mathbb{Z}_2$ given by the generating power serie:$S(X) = \frac{Q(x)}{P(X)} = \sum_{i \in \mathbb{N}} s_i X^i$ where:

$$P(X) = 1 + X^5 + X^6 + X^7 \text{ and } Q(X) = 1 + X + X^4 + X^5$$

1. Compute the first 14 values of the sequence.

2. Assuming that 7 is an upper bound on the linear complexity, compute the minimal polynomial of s.

III Implementation

Implement the basic operations of an LFSR including:

1. Given the initial state and connection polynomial of the LFSR, compute the feedback bit at position N.

2. Given the first $2n$ values of the LFSR output sequence, where n is an upper bound on the linear complexity of the LFSR, compute the minimal polynomial of the output sequence.