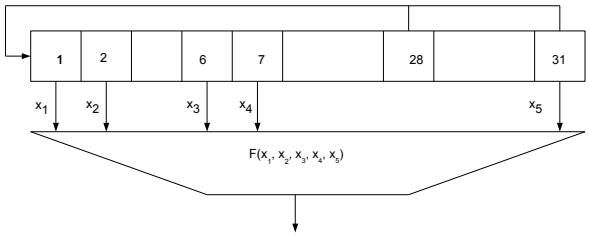
MANDATORY EXERCISE 2



A filter generator is given: LFSR of length 31 with characteristic polynomial $X^{31}+X^3+1$ and Boolean function $F(x_1, x_2, x_3, x_4, x_5) = x_1x_2 + x_3 + x_4 + x_5$.

Given key-stream of length $N = 100$, compute the initial state with Fast Correlation attack. Key-stream:

$$1,0,1,1,1,0,1,0,0,1,0,1,1,0,0,1,0,0,1,0,1,1,0,0,1,0,0,1,1,0,$$
$$0,0,1,1,0,1,0,0,0,1,0,0,1,0,0,0,0,0,1,0,0,1,0,0,0,0,1,0,1,1,$$
$$1,0,0,0,1,0,1,1,0,0,0,0,0,1,0,0,1,0,0,0,0,0,1,0,1,0,1,0,1,0,$$
$$0,1,1,0,1,0,0,1,1,0$$

You should provide a short description of the attack, find good affine approximation for F, compute posterior probabilities of zero-relations and choose linear equations with low weight left-hand side, solve them. The deadline is Sunday, 6 April, 2014.