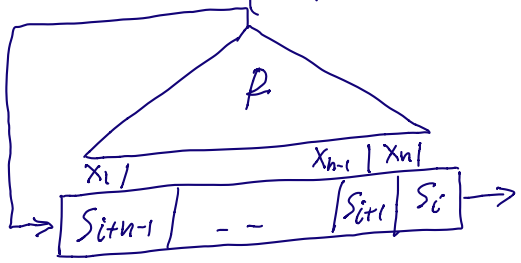
Nonlinear Feedback Shift Registers and stream cipher Grain.

NFSR = Register + Boolean function (used for the feedback)



$f = f(x_1 \dots x_n)$

$s_{i+n} = f(s_{i+n-1}, \dots, s_i)$

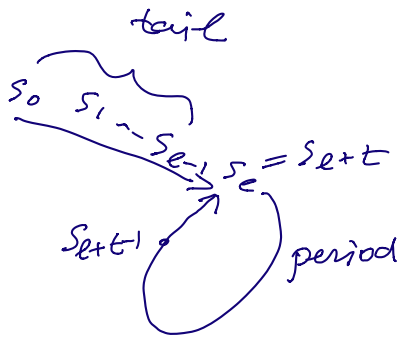
LFSR is a particular case of NFSR

where feedback $f = c_1 \cdot x_1 + \dots + c_{n-1} x_{n-1} + c_n x_n$.

$s_0 = (s_{n-1} \dots s_1 s_0)$ initial state

sequence of bits $s_0 s_1 \dots$

of states $s_0, s_1, \dots$

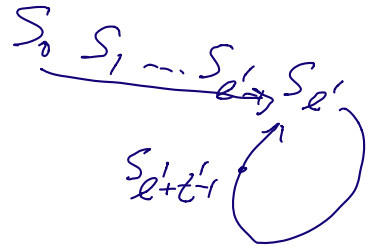


min. tail length ℓ

period length t

ℓ'

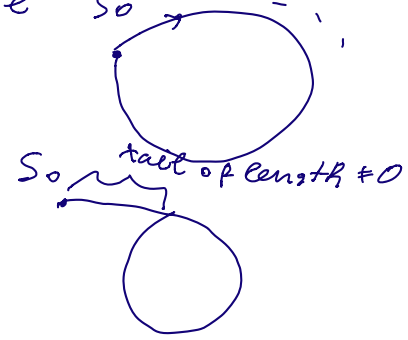
t'



Lemma. $\ell = \ell', \ t = t'$

NFSR is non-singular if
$\ell = 0$ for any initial state.

graph of state S_0 S_1 ... pure periodic
non-sing.



sing aperiodic

Lemma. NFSR is non-singular
$\Leftrightarrow$ $f(X_1 \dots X_n) = X_n + g(X_1 \dots X_{n-1})$

Proof. NFSR is non-singular
$\Leftarrow$ every state has at most 1 previous state.

represent $f = \underbrace{h(X_1 \dots X_{n-1}) \cdot X_n}_{\text{all ANF terms which depend on } X_n} + \underbrace{g(X_1 \dots X_{n-1})}_{\text{terms which do not depend on } X_n}$

1) $h = 1$

some state $S = (S_{n-1} \dots S_1 S_0)$

any previous state is

$(S_{n-2} \dots S_1 S_0 X)$

$\rightarrow (\underbrace{X + g(S_{n-2} \dots S_0)}_{\| \; S_{n-1}}, S_{n-2} \dots S_1 S_0)$

$\Rightarrow$ x is unique

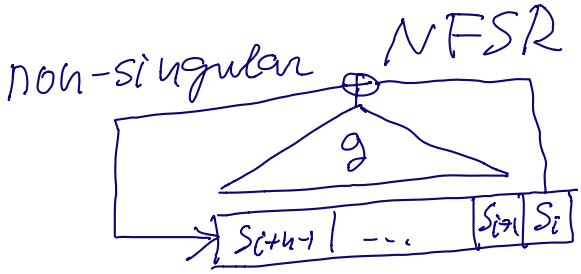
2) $k \neq 1$ find $R(v_{n-1} \dots v_1) = 0$

two states

$(v_{n-1} \dots v_1\ 0) \rightarrow (g(v_{n-1} \dots v_2), v_{n-1} \dots v_1)$

$(v_{n-1} \dots v_1\ 1) \rightarrow (g(v_{n-1} \dots v_2), v_{n-1} \dots v_1)$

We have constructed a state with 2 previous states on the graph of NFSR states. ▨



$$s_{i+n} = s_i + g(s_{i+n-1}, \dots, s_{i+1})$$

---

de Bruijn NFSR

if its min period is 2^n.

(in LFSR max. poss. period is $2^n - 1$)

Example $n=3$, $f(x_1 x_2 x_3) = 1 + x_2 + x_3 + x_1 x_2$ (non-singular)

x_1	x_2	x_3	f
0	0	0	1
1	0	0	1
1	1	0	1
1	1	1	0
0	1	1	1
1	0	1	0
0	1	0	0
0	0	1	0
0	0	0	

min. period is $2^3 = 8$

NFSR(f) is de Bruijn.

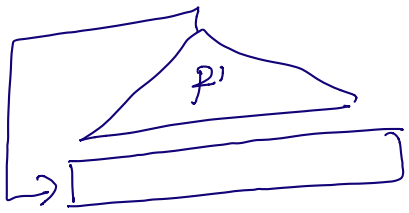
How to construct de Bruijn NFSRs.

LFSR $f(x_1 \cdots x_n) = c_1 \cdot x_1 + \cdots + c_n x_n \quad (c_n = 1)$

modify LFSR into NFSR

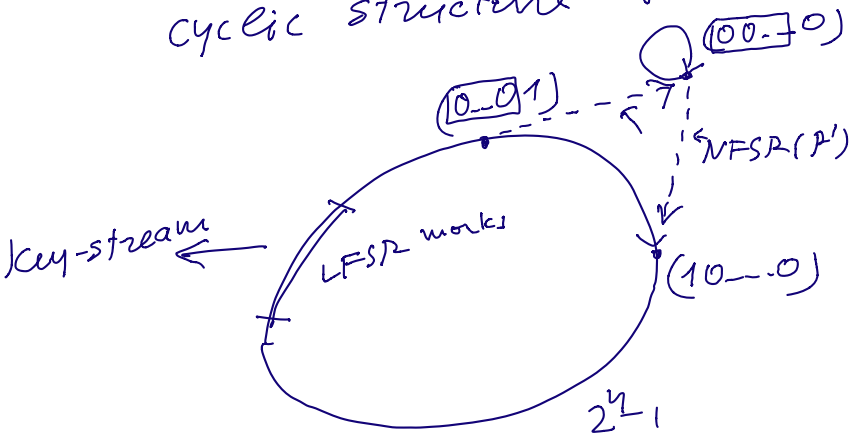
assume LFSR is of period $2^n - 1$

$$f'(x_1 \cdots x_n) = f(x_1 \cdots x_n) + (x_1 + 1)(x_2 + 1)\cdots(x_{n-1} + 1)$$



de Bruijn

cyclic structure of the LFSR



$$f'(s_{n-1} \cdots s_1 s_0) = \begin{cases} f(s_{n-1} \cdots s_1 s_0) & (s_{n-1} \cdots s_1) \neq (0 \cdots 0) \\ f(s_{n-1} \cdots s_1 s_0) + 1 & (s_{n-1} \cdots s_2) = (0 \cdots 0) \end{cases}$$

$$f'(0 \cdots 0*) \neq f(0 \cdots 0*)$$

NFSR(f') is de Bruijn.

A more general method of constructing de Bruijn NFSR.

NFSR(R) non-singular

$x = (s_{n-1} \dots s_1 s_0) \longrightarrow y = (s_n s_{n-1} \dots s_1)$

$\bar{x} = (s_{n-1} \dots s_1 \bar{s}_0) \longrightarrow \bar{y} = (\bar{s}_n, s_{n-1}, \dots, s_1)$

modify feedback function

$$f' = f + (x_1 + s_{n-1} + 1)(x_2 + s_{n-2} + 1) \cdots (x_{n-1} + s_1 + 1)$$

$$= \begin{cases} f & \text{if } (x_1 \dots x_{n-1}) \neq (s_{n-1} \dots s_1) \\ f+1 & = \end{cases}$$

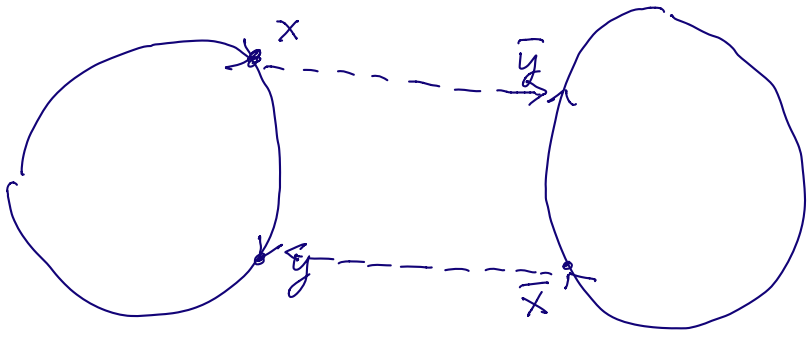
NFSR(R')

$x = (s_{n-1} \dots s_1 s_0) \longrightarrow \bar{y} = (\bar{s}_n s_{n-1} \dots s_1)$

$\bar{x} = (s_{n-1} \dots s_1 \bar{s}_0) \longrightarrow y = (s_n s_{n-1} \dots s_1)$

What happens with cyclic structure

1) $x, \bar{x}$ are on different cycles in NFSR(R) graph of states

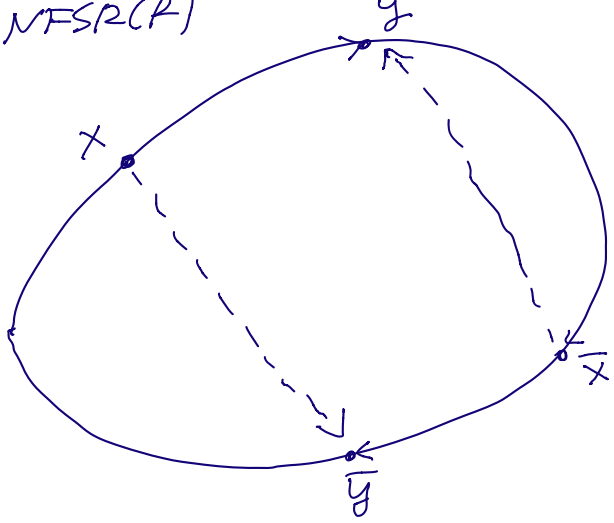


NFSR(R')

glue two cycles but all other cycles are intact.

2) $x, \bar{x}$ are on the same cycle

NFSR(F)



NFSR(F')

the cycle got split into two cycles.

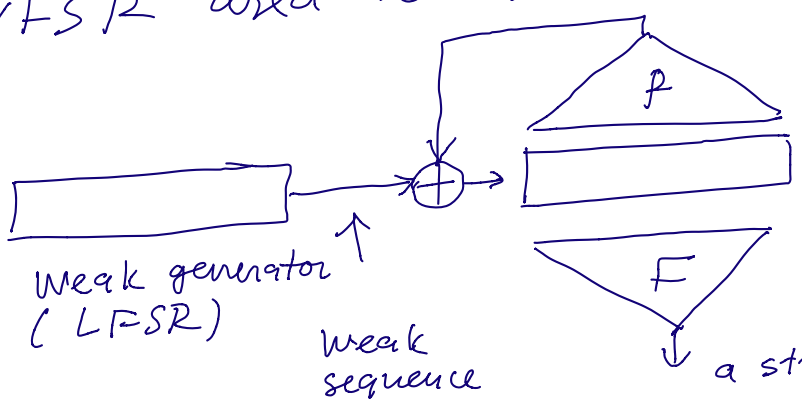
Hard research problems

1) Construct de Bruijn NFSR(F)
where deg f is low (2, 3, ..)

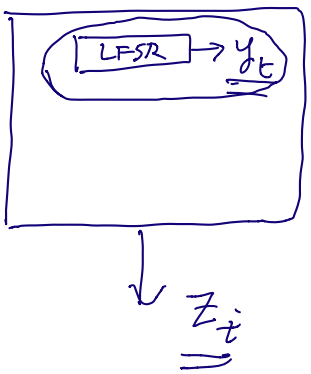
2) given $\underline{a}$ and NFSR(F)
if there is a cycle of length $\leq a$.

Stream cipher Grain and correlation attack.

NFSR used to make bit seq. stronger.



correlation attack.



assume

$Pr(y_t = z_t) = q \neq \frac{1}{2}$

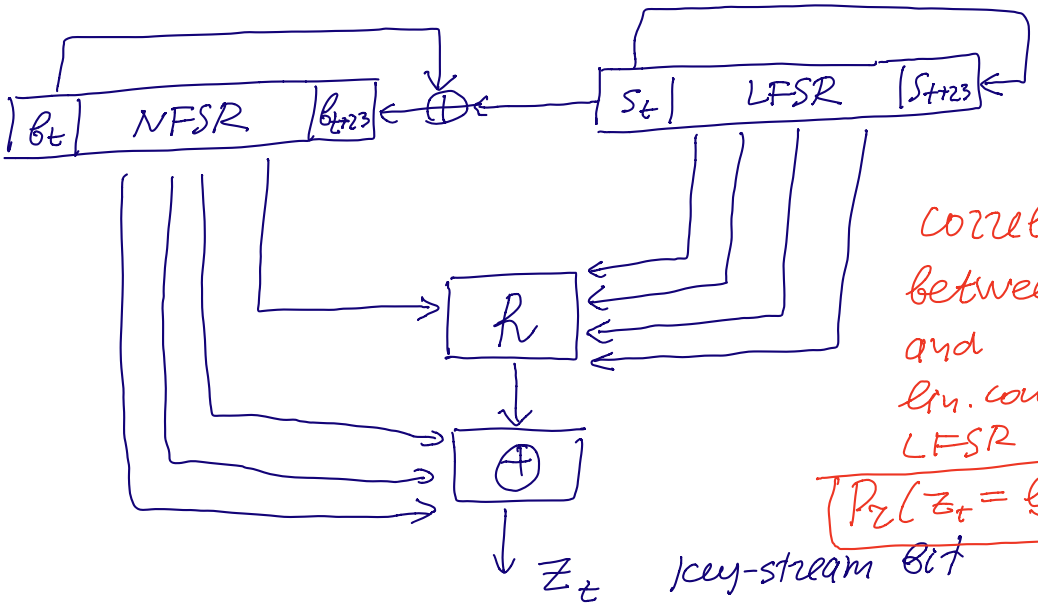
task $z^N = z_0 \dots z_{N-1}$

find LFSR initial state.

z_t key-stream

Grain finalist to the European Stream Cipher Competition (eStream)

1. Toy version of Grain



correlation between z_t and lin. comb. of LFSR bits

$Pr(z_t = \text{lin.comb.}) \neq \frac{1}{2}$.

LFSR feedback

$$s_{t+24} = s_t + s_{t+1} + s_{t+2} + s_{t+7}$$

($x^{24} + x^7 + x^2 + x + 1$ prim. gen. polynomial)

NFSR feedback. non-linear

$$b_{t+24} = s_t + b_t + b_{t+5} + b_{t+14} + b_{t+20} b_{t+21} + b_{t+11} b_{t+13} b_{t+15}$$

key stream

$$z_t = h(s_{t+3}, s_{t+7}, s_{t+17}, s_{t+19}, b_{t+7}) + \sum_{j=1,3,8} b_{t+j}$$

Boolean function

$$R(X_0X_1X_2X_3X_4) = X_1+X_4+X_0X_3+X_2X_3+X_3X_4+X_0X_1X_2 + X_0X_2X_3+X_0X_2X_4+X_1X_2X_4+X_2X_3X_4$$

Properties of R.

1) correlation immune of order 1.

$$Pr(R=x_i) = \frac{1}{2} \quad i=0,\dots,4$$

2) WH spectrum is rather flat.

Finding correlation between Z_t and LFSR bits.

$$Z_t = \sum_{i=0,5,14,24} z_{t+i}$$

two equation from the definition

1) $$Z_t = \sum_{i=0,5,14,24} R(S_{t+3+i}, S_{t+7+i}, S_{t+15+i}, S_{t+19+i}, S_{t+17+i}) + \sum_{j=1,3,8} S_{t+j} = \sum_{j=1,3,8} S_{t+20+j}\cdot S_{t+21+j} + S_{t+11+j}\cdot S_{t+13+j}\cdot S_{t+15+j}$$

2) $$S_{t+17} + \sum_{i=0,5,14,24} S_{t+17+i} = S_{t+37}S_{t+38} + S_{t+28}\cdot S_{t+30}\cdot S_{t+32}$$

vector of LFSR bits

$$A_t = (S_{t+3}, S_{t+7}, S_{t+15}, \dots, S_{t+43}, S_{t+1}+S_{t+3}+S_{t+8})$$

all bit of LFSR which are in 1) and 2).

Find distribution on A_t conditioned by 1), 2)

$$Pr(A_t = a/1),2))$$

vector $P = (P_0\ P_1 \ldots P_{2^{17}-1})$

apply WH transform to P.

get all correlations like

$$Pr\left(\underbrace{S_{t+7}+S_{t+19}+S_{t+12}+S_{t+24}+S_{t+17}+S_{t+21}+S_{t+31}}_{+\ S_{t+43}+S_{t+1}+S_{t+3}+S_{t+8}} = Z_t\right) = \frac{1}{2} + \delta$$

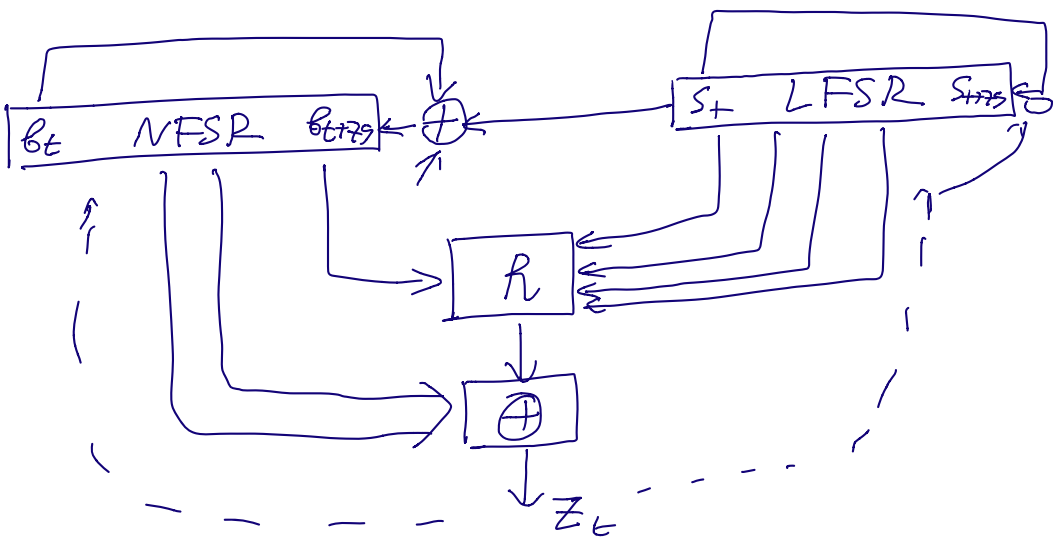
$$2|\delta| = 2^{-9.83007\ldots}$$

⇒ find initial state of the LFSR

$$N \geq \frac{t_\alpha^2}{\delta^2} > 2^{21}$$

⇒ method is not very efficient.

Large Grain v 1.

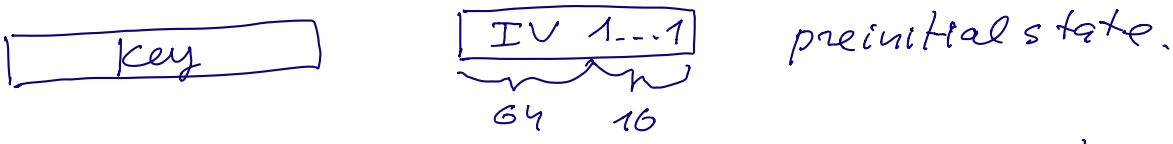


NFSR Feedback Boolean function of degree 6

Initialization

key length = 80 bits

IV length = 64 bits.



preinitial state.

cipher clocks 160 times without generating key-stream.

Then key-stream generated and data encrypted.