Linear feedback shift registers

LFSR fixed parameters ℓ, $c_1, c_2, \dots, c_\ell$

from seed $(x_1, x_2, \dots, x_\ell)$ generate

$$x_{n+\ell} \equiv c_1 x_{n+\ell-1} + c_2 x_{n+\ell-2} + \dots + c_\ell x_n \pmod 2$$

$$PRG((x_1, x_2, \dots, x_\ell)) = x_{\ell+1}\, x_{\ell+2}\, x_{\ell+3} \dots$$

real world glibc uses $x_{n+31} \equiv x_{n+28} + x_n \pmod 2$

comments

- LFSRs are easy to predict ($\Rightarrow$ unsuitable for crypto)
- very easy to implement in hardware

EG stream cipher using LFSR $x_{n+3} \equiv x_{n+2} + x_n \pmod 2$

$k = (100)_2 \qquad m = (101\ 111\ 001)_2$

$x_1 = 1 \quad x_2 = 0 \quad x_3 = 0$

$PRG((x_1, x_2, x_3)) = x_4 x_5 x_6 \dots$

$= 111, 010, 011$

$x_4 = x_3 + x_1 \equiv 1 \pmod 2$

$x_5 = x_4 + x_2 \equiv 1$

$x_6 = x_5 + x_3 \equiv 1$

$x_7 \equiv 0 \quad x_8 \equiv 1 \quad x_9 \equiv 0$ $\longrightarrow$ repeats

$x_{10} \equiv 0 \quad x_{11} \equiv 1 \quad x_{12} \equiv 1$

$c = m \oplus PRG$

m	101	111	001
$\oplus$ PRG	111	010	011
$= c$	010	101	010

EG $c = (111\ 111\ 111)_2$

Eve knows: stream cipher with $x_{n+3} \equiv x_{n+2} + x_n \pmod 2$

$m = (110\ 0\dots)_2$

$c = m \oplus PRG$

$PRG = c \oplus m$ (1111... , 1100...)

$= 0011\dots$ ($x_4 x_5 x_6 x_7 \dots$)

$x_4 = 0 \quad x_5 = 0 \quad x_6 = 1$

$x_7 = x_6 + x_4 \equiv 1 \pmod 2 \qquad x_8 \equiv 1, \dots$

c	111	111	111
$\oplus$ PRG	001	110	100
$= m$	110	001	011