# Content scramble system

**CSS** used for encryption of DVDs
combines 2 LFSRs (nonlinearly!)

introduced 1996
broken 1999

**baby CSS**

LFSR-1 $x_{n+3} \equiv x_{n+1} + x_n \pmod 2$

LFSR-2 $x_{n+4} \equiv x_{n+2} + x_n \pmod 2$

CSS-PRG : add outputs from LFSRs **with carry**
(nonlinear)

**EG** (0,0,1)
(0,1,0,1) seeds for LFSRs

→ repeats after $2^3-1$ bits

| | | seed | output | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | LFSR-1 | 0 0 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | ... |
| + | LFSR-2 | 0 1 0 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | ... |
| | carry | | | | | | 1 | | | | |
| = | CSS-PRG | | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | ... |

**comments**

- less predictable than single LFSR

  initial output 0 1 ... could have come from

  $$\begin{array}{r} 01\ldots \\ +\ 00\ldots \end{array} \quad \begin{array}{r} 10\ldots \\ +\ 10\ldots \end{array} \quad \begin{array}{r} 11\ldots \\ +\ 11\ldots \end{array} \quad \begin{array}{r} 00 \\ +\ 01\ldots \end{array}$$

  don't learn about states of LFSRs but about their correlation

- the carry is crucial

  $$\begin{array}{lll} & \text{LFSR-1} & a_1 \quad a_2 \quad \ldots \\ + & \text{LFSR-2} & b_1 \quad b_2 \quad \ldots \\ \hline \end{array}$$

  without carry $a_1+b_1 \quad a_2+b_2 \quad \ldots$ (addition mod 2)

  nonlinear!

  with carry $a_1+b_1 \quad a_2+b_2+a_1b_1$ (mod 2)

  carry $\Leftrightarrow$ $a_1=1$ and $b_1=1$ $\Leftrightarrow$ $a_1b_1 \equiv 1 \pmod 2$