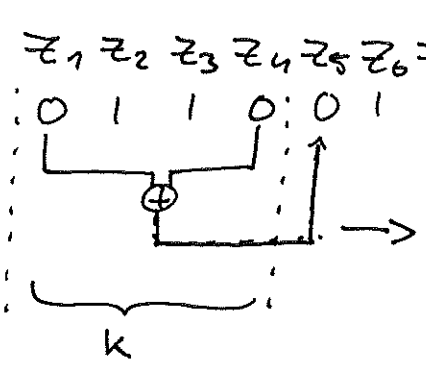
Ex 22: Linear Feedback Shift Register (LFSR) based stream cipher

(c) $n = 4$, $\underbrace{s_1 = s_4 = 1,\ s_3 = s_2 = 0}_{s = 1001}$, $\ell = 20$, $k = 0110$

z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}	z_{11}	z_{12}	z_{13}	z_{14}	z_{15}	z_{16}	z_{17}	z_{18}	z_{19}	z_{20}
0	1	1	0	0	1	0	0	0	1	1	1	1	0	1	0	1	1	0	0

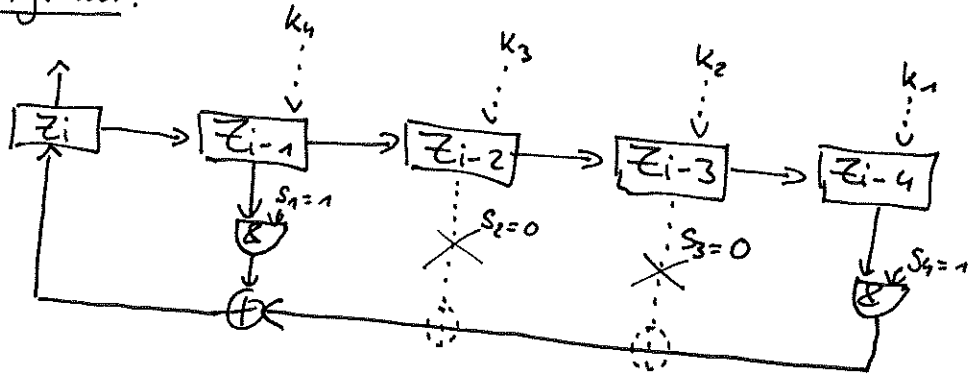


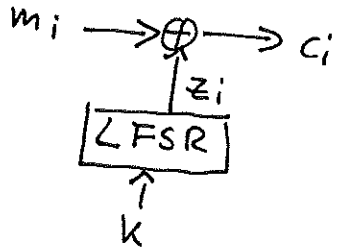
$$z_i = \sum_{j=1}^{4} s_j z_{i-j} \equiv z_{i-1} \oplus z_{i-4}, \quad 4 < i < 20$$

Encryption:

m	1011	0001	0100	1101	0100
⊕					
z	0110	0100	0111	1010	1100
c	1101	0101	0011	0111	1000

block diagram:





(d) period is 15, c.f. stream $z_1 \ldots z_{20}$ in (c)

// all zero case is invalid

⇒ period is maximal since $n = 4$ register can only have $2^4 - 1$ states

⇒ $p_{max} = p = 2^4 - 1 = 15$

Background info:

- multiple LFSRs are used in $\left\{\begin{matrix}\text{GSM}\\\text{Bluetooth}\\\text{DVB-T}\end{matrix}\right\}$ due to easy implementation

correction: $p = \min\{K \in \mathbb{N} \mid \exists i_0 \in \mathbb{N}, i \in \mathbb{N}, \forall i \geq i_0 : z_{i+K} = z_i\}$

$\Rightarrow$ will be explained in the next homework