College Cryptografie

Cursusjaar 2007

Schuifregisters

28 januari 2007

Stroomvercijfering

Schuifregister

LFSR

Periode LFSR

Kwaliteit LFSR

Niet-lineaire systemen

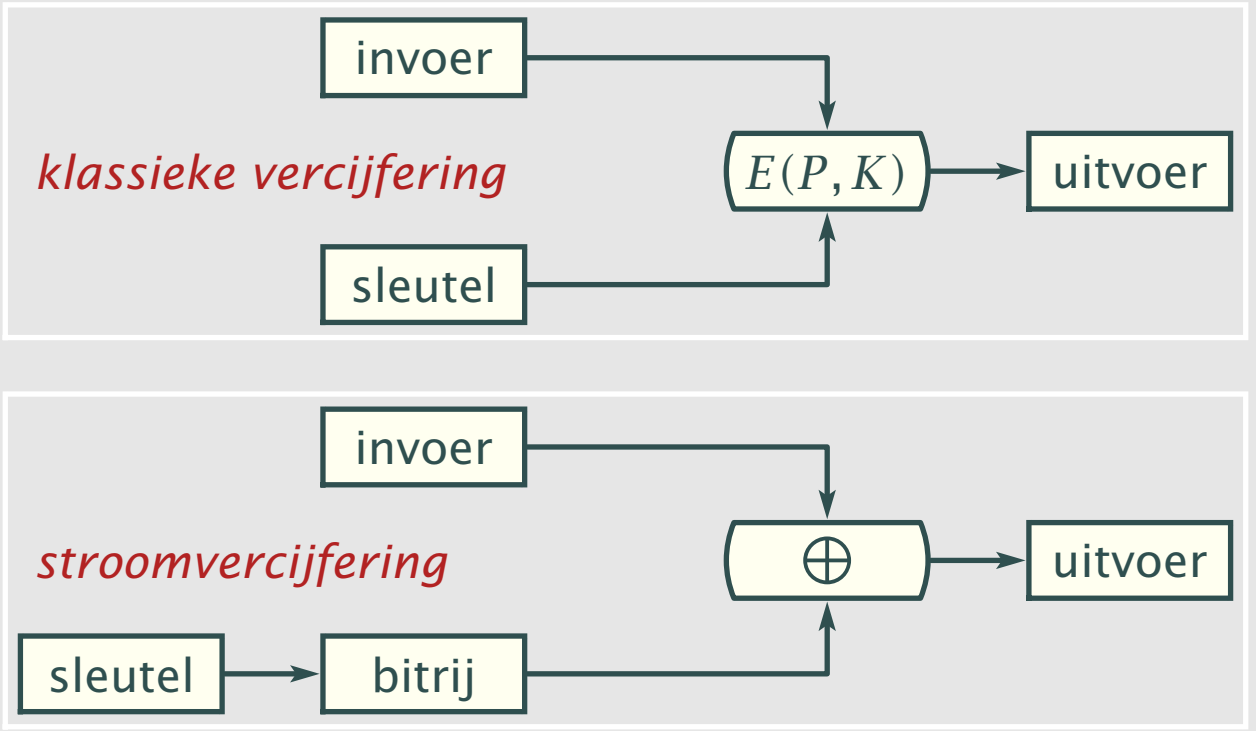
Lineaire complexiteit

Filtering

LFSR-combinatie

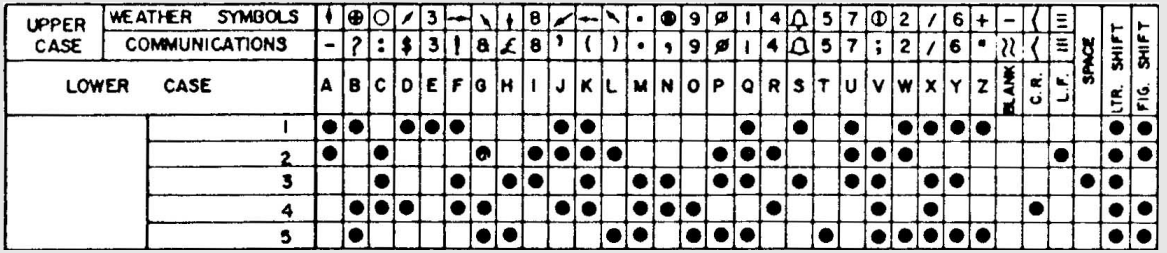
Correlatie-aanval

Kloksturing



Stroomvercijfering

Baudot code voor telexverkeer



Gilbert S. Vernam, 1917

telexcode + sleuteltape

Tweede Wereldoorlog, Wehrmacht-Führer hoofdkwartier

Lorentz Schlüsselzusatz SZ-40/42

Siemens Geheimschreiber T52-a/e

Vernam vercijfering

vercijfering en ontcijfering

ASCII	H	a	l	l	o
P	01001000	01100001	01101100	01101100	01101111
S	01100111	10101000	01000110	11010011	01000010
$C = P \oplus S$	00101111	11001001	00101010	10111111	00101101
C	00101111	11001001	00101010	10111111	00101101
S	01100111	10101000	01000110	11010011	01000010
$P = C \oplus S$	01001000	01100001	01101100	01101100	01101111
ASCII	H	a	l	l	o

reconstructie sleutelstroom

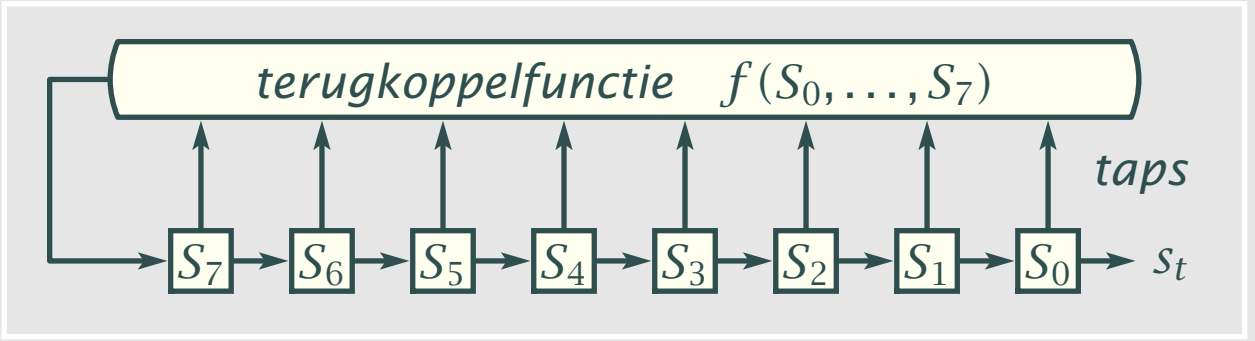
C	00101111	11001001	00101010	10111111	00101101
P	01001000	01100001	01101100	01101100	01101111
$S = C \oplus P$	01100111	10101000	01000110	11010011	01000010

Golomb criteria (standaardwerk: *Shift Register Sequences*)

- aantal enen en nullen (zo goed mogelijk) gelijk
- run = rij dezelfde bits, blok = rij 1'en, gat = rij 0'en
  evenveel gaten als blokken van dezelfde lengte
  frequentie gaten en blokken neemt af met de lengte
- uitfase-autocorrelatie is constant

$$C(\delta) = 1 - \frac{2}{p} \sum_{i=0}^{p-1} s_i \oplus s_{i+\delta} \quad \delta = 0, 1, \ldots, p-1 \quad p = \text{ periode}$$

Kwaliteit sleutelstroom



opeenvolging: $S_0S_1S_2S_3S_4S_5S_6S_7(t-1) \rightarrow S_0S_1S_2S_3S_4S_5S_6S_7(t)$

opbouw bituitvoer: $\ldots s_{t-2}\, s_{t-1} \rightarrow \ldots s_{t-2}\, s_{t-1}\, s_t$

$s_t = S_0(t),\ S_0(t) = S_1(t),\ \ldots,\ S_7(t) = f(S_0,\ldots,S_7)(t)$

Schuifregister

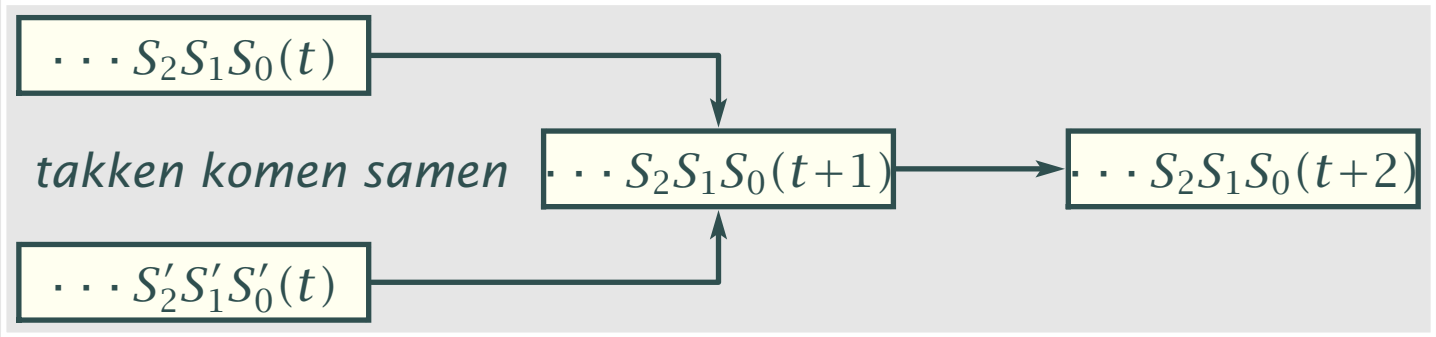
Terugkoppelfunctie van n-trapsregister $f(S_0, S_1, \ldots, S_{n-1})$

- voorbeeld: $f = 1 + S_0 + S_1S_3 + S_2S_4 + S_1S_2S_3S_4$
- algebraïsche normaalvorm

  $$f(S) = 1 + S_0 + \cdots + S_n + S_0S_1 + \cdots + S_{n-2}S_{n-1} + S_0 \ldots S_{n-1}$$

- er zijn 2^{2^n} terugkoppelfuncties voor n-traps register
- bepaal terugkoppelfunctie uit verzameling registerwaarden
- losse cycli en vertakkingen mogelijk
- deBruin rij heeft maximale periode 2^n, aantal $2^{2^{n-1}-n}$

Geen vertakkingen → alleen gesloten cycli



Vlak voor samenkomst geldt

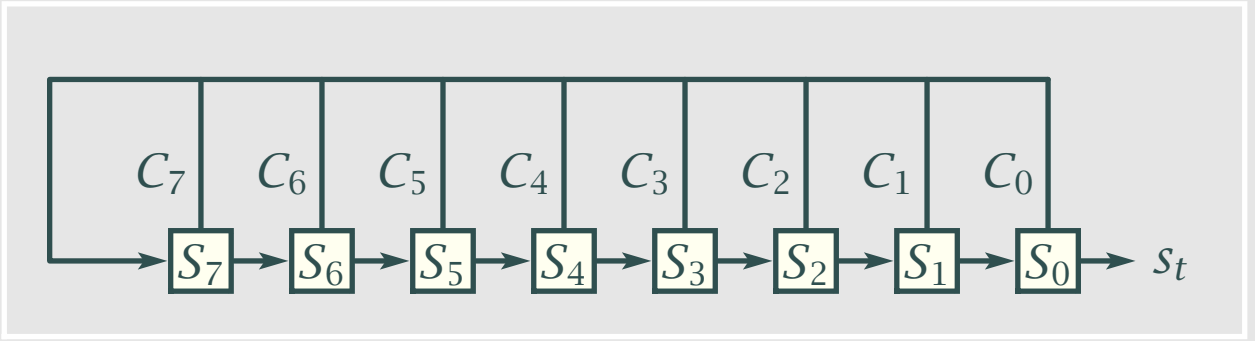
$$S_0 \neq S'_0,\ S_i = S'_i, i > 0$$

Vertakkingen ontbreken *iff*

$$f(S_0S_1S_2\ldots) = S_0 + f(S_1S_2\ldots)$$

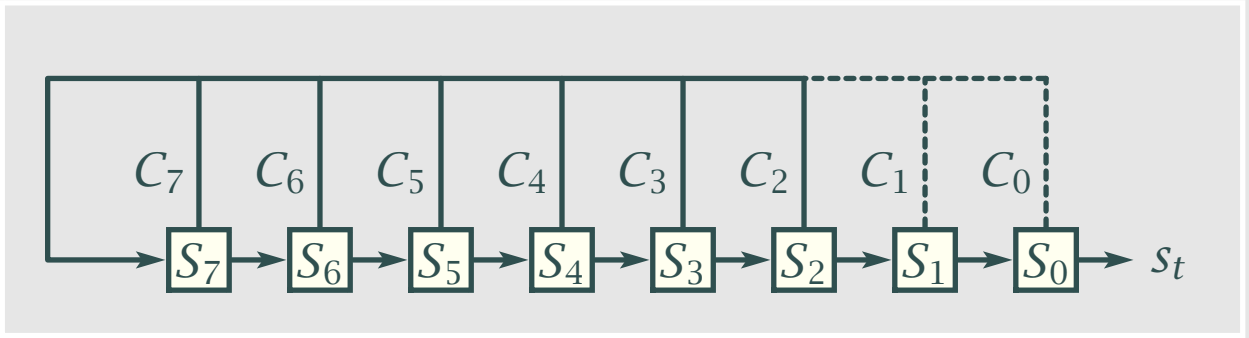
S_0	S_1	S_2	$f(S)$	bijdrage tot $f(S)$
0	0	0	0	$0 \cdot (S_0+1)(S_1+1)(S_2+1)$
0	0	1	0	$0 \cdot (S_0+1)(S_1+1)S_2$
0	1	0	0	$0 \cdot (S_0+1)S_1(S_2+1)$
0	1	1	1	$1 \cdot (S_0+1)S_1S_2$
1	0	0	0	$0 \cdot S_0(S_1+1)(S_2+1)$
1	0	1	1	$1 \cdot S_0(S_1+1)S_2$
1	1	0	1	$1 \cdot S_0S_1(S_2+1)$
1	1	1	1	$1 \cdot S_0S_1S_2$

$$
\begin{aligned}
f &= (S_0+1)S_1S_2 + S_0(S_1+1)S_2 + S_0S_1(S_2+1) + S_0S_1S_2 \\
&= S_0S_1S_2 + S_1S_2 + S_0S_1S_2 + S_0S_2 + S_0S_1S_2 + S_0S_1 + S_0S_1S_2 \\
&= S_1S_2 + S_0S_2 + S_0S_1
\end{aligned}
$$



$$f(S) = C_0S_0 \oplus C_1S_1 \oplus \cdots \oplus C_{n-1}S_{n-1}$$
$$= \sum_{i=0}^{n-1} C_iS_i \qquad C_i \in \{0,1\}$$

$$\ldots s_{t-2}s_{t-1}s_t \rightarrow s_t = C_{n-1}s_{t-1} \oplus \cdots \oplus C_0s_{t-n} = \sum_{i=1}^{n} C_{n-i}s_{t-i}$$



- als $C_0 = C_1 = 0$ verkorting tot vertraagd 6-traps register
  als regel daarom $C_0 = 1$

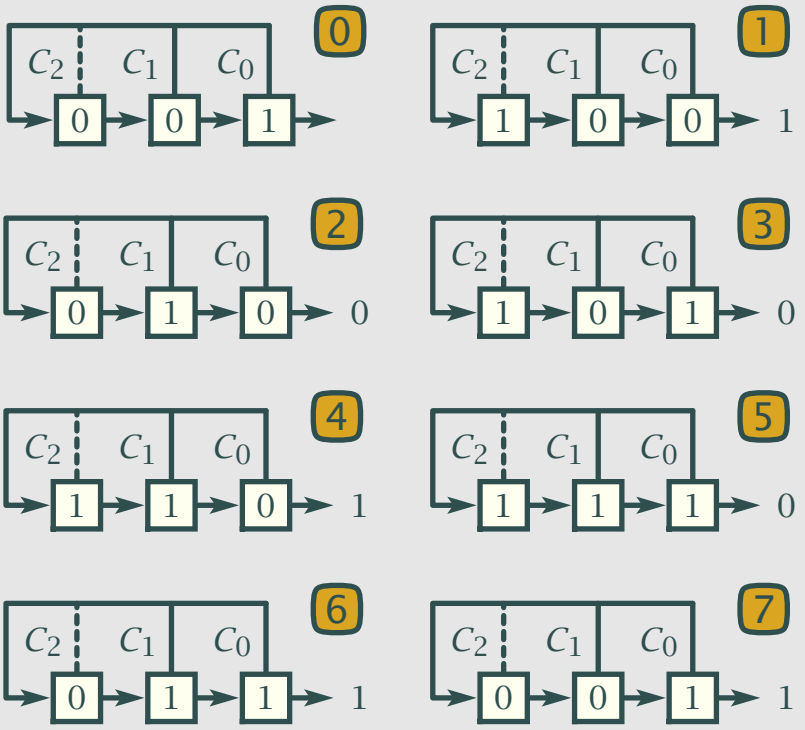
- als $S_0 = S_1 = \cdots = S_{n-1} = 0$ dan $s_t = 0$ voor alle t
  er zijn $2^n - 1$ registertoestanden $\neq 0 \ldots 0$
  dus maximale periode $2^n - 1$

-

t	$S_2S_1S_0$	s_t
0	001	
1	100	1
2	010	0
3	101	0
4	110	1
5	111	0
6	011	1
7	001	1

- maximaalrij (1001011)
  $p = 2^n - 1 = 2^3 - 1 = 7$

$$f(x) = 1 + x + x^3$$

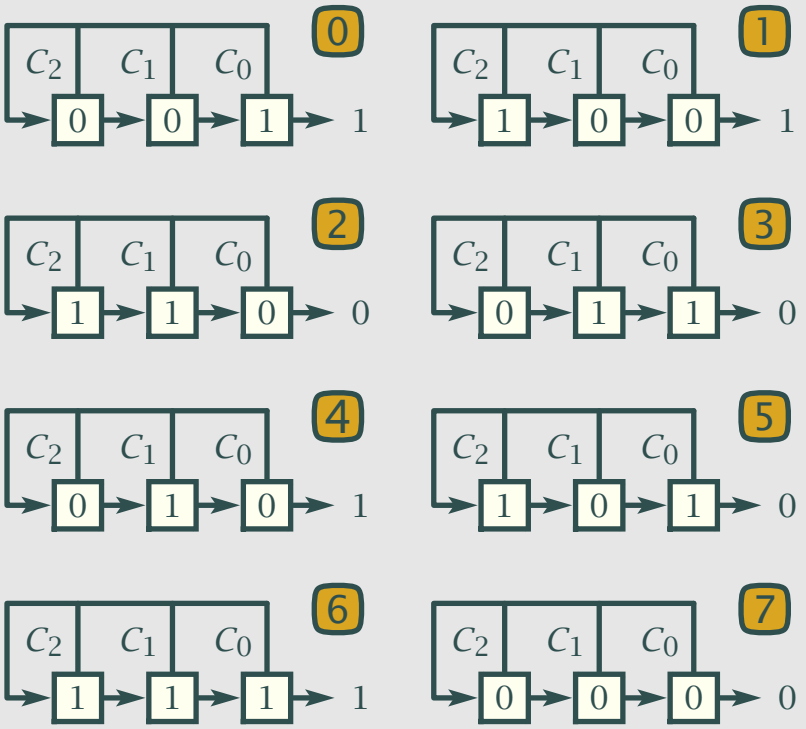


Voorbeeld LFSR

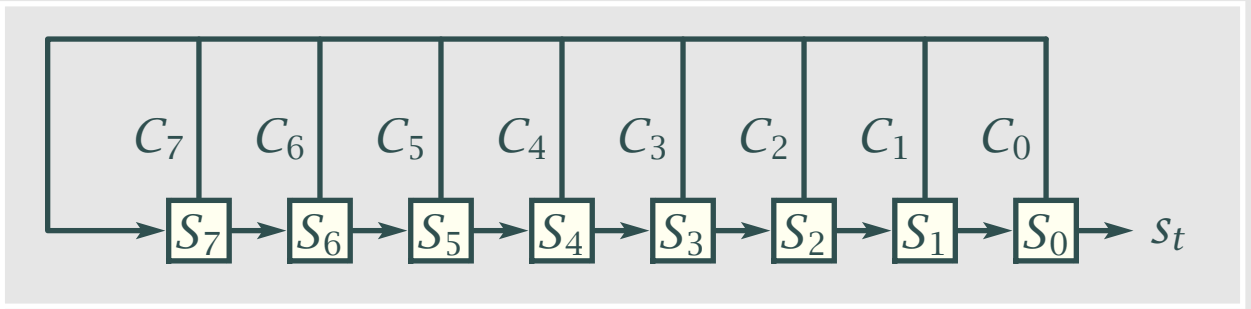
t	$S_2S_1S_0$	s_t
0	001	1
1	100	1
2	110	0
3	011	0
4	010	1
5	101	0
6	111	1
7	000	0

- $p = 4$ rij (1100)
  $p = 2$ rij (10)
  $p = 1$ rij (1) (0)

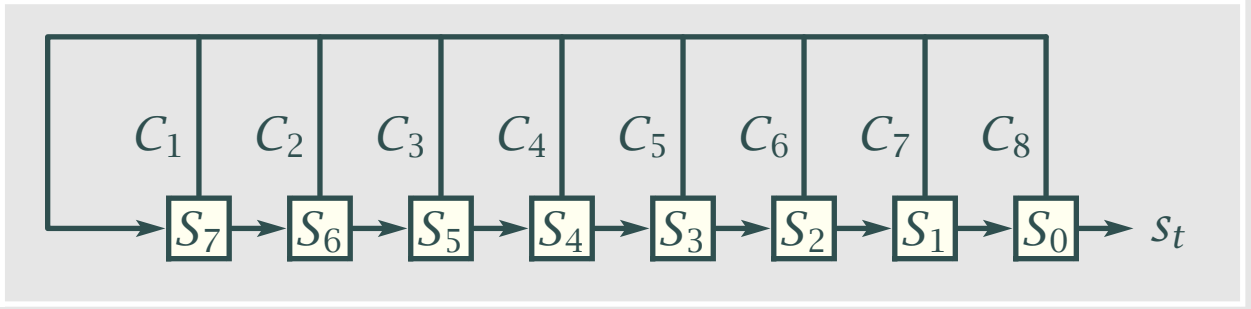
$$f(x) = 1 + x + x^2 + x^3$$



Voorbeeld LFSR



$$f(S) = \sum_{i=0}^{n-1} C_i S_i \qquad s_t = \sum_{i=1}^{n} C_{n-i} s_{t-i}$$



$$f(S) = \sum_{i=1}^{n} C_i S_{n-i} \qquad s_t = \sum_{i=1}^{n} C_i s_{t-i}$$

Alternatieve nummering

genererende functie is machtreeks $G(x) = \sum_{t=0}^{\infty} s_t x^t$

$$
\begin{aligned}
G(x) &= \sum_{t=0}^{\infty} x^t \sum_{i=1}^{n} C_{n-i} s_{t-i} = \sum_{i=1}^{n} C_{n-i}\, x^i \sum_{t=0}^{\infty} s_{t-i} x^{t-i} \\
&= \sum_{i=1}^{n} C_{n-i}\, x^i \{ s_{-i} x^{-i} + \cdots s_{-1} x^{-1} + \cdots + s_t x^t + \cdots \} \\
&= \sum_{i=1}^{n} C_{n-i}\, x^i \{ s_{-i} x^{-i} + \cdots s_{-1} x^{-1} + G(x) \}
\end{aligned}
$$

$G(x)$ oplossen uit deze vergelijking

$$G(x) = \frac{\sum_{i=1}^{n} C_{n-i} x^i \{s_{-i} x^{-i} + \cdots + s_{-1} x^{-1}\}}{\sum_{i=0}^{n} C_{n-i} x^i}$$
$$= \frac{s(x)}{f(x)}$$

- teller hoogstens van graad $n-1$, noemer van graad n
- teller representeert begintoestand
- noemer onafhankelijk begintoestand: *karakteristieke functie*
- met alternatieve nummering *reciprook polynoom* verkregen
  $f^*(x) = x^n f(x^{-1})$

$$G(x) = \sum_{t=0}^{\infty} s_t x^t = \sum_{k=0}^{\infty} \sum_{i=0}^{p-1} s_{i+k.p} x^{i+k.p}$$
$$= (s_0 + s_1 x + \cdots + s_{p-1} x^{p-1})(1 + x^p + x^{2p} + \cdots)$$
$$= (s_0 + s_1 x + \cdots + s_{p-1} x^{p-1})(1 - x^p)^{-1}$$
$$= \frac{s(x)}{f(x)} = \frac{1}{f(x)} \quad \text{(kies } s(x) \text{ geschikt)}$$

$$f(x)(s_0 + s_1 x + s_2 x^2 + \cdots + s_{p-1} x^{p-1}) = 1 - x^p$$

Kleinste p waarvoor $f(x)$ een deler van $1 - x^p$ is een periode

Periode LFSR

Periode maximaal *iff* karakteristiek polynoom $f(x)$ irreducibel

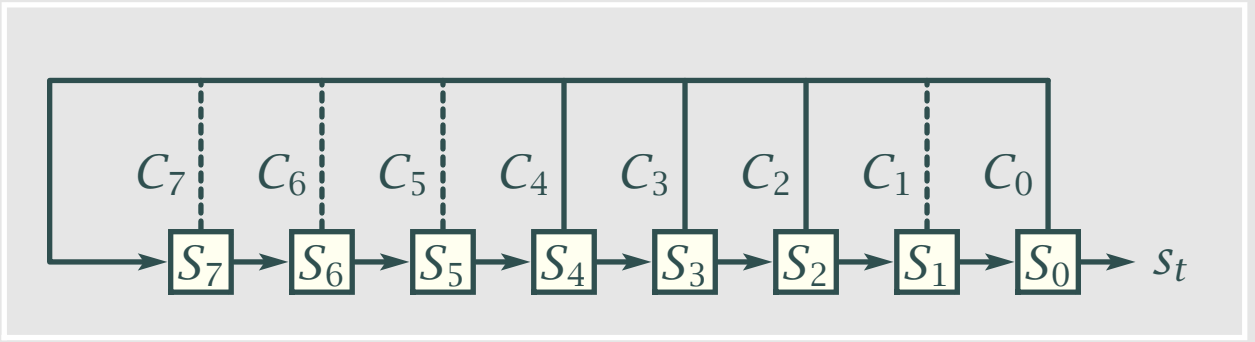
$$\text{Stel } f(x) = g(x)h(x) \text{ dan } \frac{1}{f(x)} = \frac{a(x)}{g(x)} + \frac{b(x)}{h(x)}$$

graad $n_f = n_g + n_h$

maximaal $p_f = 2^{n_f} - 1, p_g = 2^{n_g} - 1, p_h = 2^{n_h} - 1$

$$\begin{aligned} p_f &\leq kgv(p_g, p_h) = 2^{n_g+n_h} - 2^{n_g} - 2^{n_h} + 1 \\ &\leq 2^{n_f} - 3 \quad (\text{wegens } n_g, n_h \geq 1) \\ &< 2^{n_f} - 1 \\ &< p_f \end{aligned}$$

Tegenspraak dus $f(x) \neq g(x)h(x)$



$$f(x) = x^8 + x^4 + x^3 + x^2 + 1$$

geschikte polynomen $\#n = \dfrac{\phi(2^n - 1)}{n}$

Karakteristieke functie LFSR

Golomb #1: aantal enen en nullen gelijk

- kijk naar het bit in S_0 in maximaalrij
- register doorloopt alle bitcombinaties behalve (00...00)
- daarvan 2^{n-1} combinaties met bit 1 in S_0
- en $2^{n-1} - 1$ combinaties met bit 0 in S_0
- verschil 1: het best mogelijke voor oneven aantal bits

LFSR voldoet aan het criterium

Golomb #2: frequentie gaten en blokken neemt af met lengte

- blok van k 1'en betekent 01 ...10
- restant $n-k-2$ bits, dus 2^{n-k-2} blokken van lengte k
- idem voor gaten 10 ...01, totaal 2^{n-k-1} runs van lengte k
- bijzondere gevallen blok van n 1'en en gat van $(n-1)$ 0'en
- totaal aantal blokken en gaten $2+\sum_{i=1}^{n-2} 2^{n-k-1} = 2^{n-1}$
- fractie als functie van lengte k is $2^{n-k-1}/2^{n-1} = 2^{-k}$

LFSR voldoet aan het criterium

Golomb # 3: uitfase-autocorrelatie is constant

- uitfase autocorrelatie is

$$C(\delta) = 1 - \frac{2}{p} \sum_{i=0}^{p-1} s_i \oplus s_{i+\delta} \quad \delta = 0, 1, \ldots, p-1$$

- gemakkelijk omdat $s \oplus s_\delta = s'$ een andere rij uit de reeks correlatie is aantal 1'en in $s' = 2^{n-1}$ voor maximaalrij

- resultaat

$$C(\delta) = 1 - \frac{2}{2^n - 1} \times 2^{n-1} = \frac{-1}{2^n - 1} \quad \text{is constant}$$

LFSR voldoet aan het criterium

Reconstructie register en begintoestand uit $2n$ bits

- bereken volgend bit uit n voorafgaande bits

$$\ldots s_{t-2}s_{t-1}s_t \;\rightarrow\; s_t = C_{n-1}s_{t-1} \oplus \cdots \oplus C_0 s_{t-n} = \sum_{i=1}^{n} C_{n-i}s_{t-i}$$

- met n opeenvolgende bits n lineaire vergelijkingen

$$\begin{pmatrix} s_1 & s_2 & \ldots & s_n \\ s_2 & s_3 & \ldots & s_{n+1} \\ . & . & \ldots & . \\ s_n & s_{n+1} & \ldots & s_{2n-1} \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ . \\ C_{n-1} \end{pmatrix} = \begin{pmatrix} s_{n+1} \\ s_{n+2} \\ . \\ s_{2n} \end{pmatrix}$$

LFSR cryptografisch onveilig

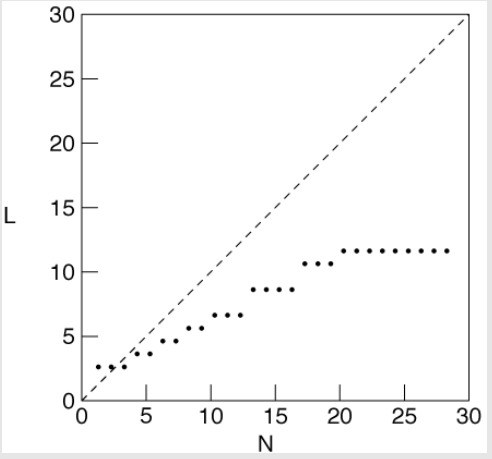
- LFSR's als bouwstenen
- Lineaire complexiteit als maat
- Bestendigheid tegen correlatie-aanval
- Filtering
  - multiplex generator
  - filterfunctie
- Registercombinaties
  - Pless, Geffe, Bruer, som generator
  - aanval via correlatie, correlatie-immuniteit
- Kloksturing
  - stop-and-go
  - krimp generator
  - A5/1 en A5/2 voor GSM's

- *lineaire complexiteit* bitrij is *equivalent LFSR*
- berekenen met Berlekamp–Massey algoritme
  start met register dat begin van de rij reproduceert
  pas het register aan als volgend bit niet goed
- voor random bitrij van n bits gemiddelde waarde $n/2+$
- lineaire complexiteit groter met meer hogere orde termen in de terugkoppelfunctie

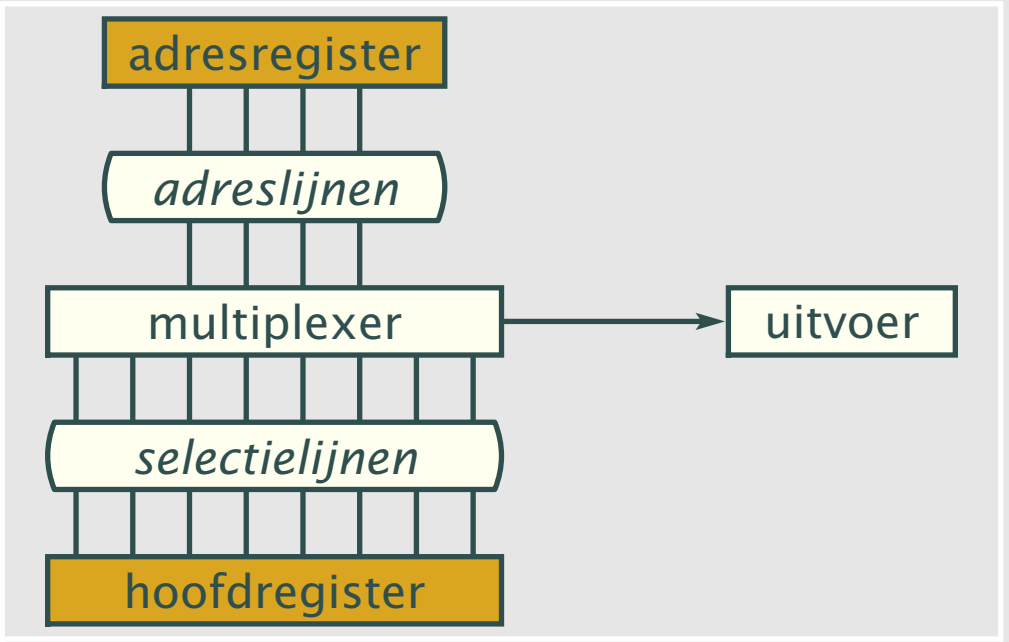
$$f(S) = S_0 + \cdots + S_0S_1 + \cdots + S_0S_1S_2 + \cdots + S_0 \ldots S_{n-1}$$

Lineaire complexiteit

s_t	$LC = f(x)$
10011110	$1 + x^3 + x^4$
$01\{100011110\}^1$	$1 + x^2 + x^3 + x^6$
$01\{100011110\}^2$	$1 + x + x^2 + x^3 + x^8 + x^9 + x^{10}$
$01\{100011110\}^*$	$x^2 + x^{11}$



Multiplex generator



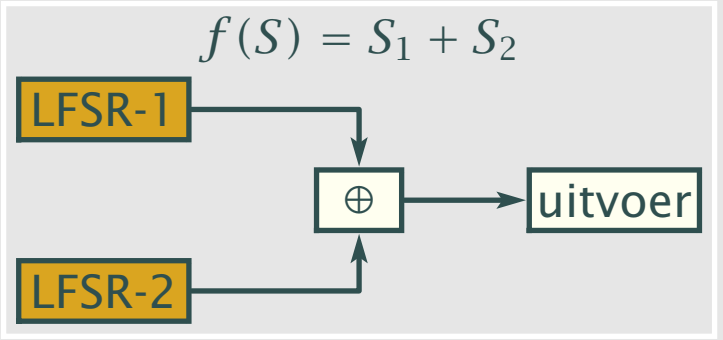
voorbeeld cryptoanalyse in syllabus

Filterfunctie op registertrappen

$$
\begin{aligned}
f_1 &= S_1 \oplus S_2 \oplus (S_1 \oplus S_3)(S_2 \oplus S_4 \oplus S_5) \oplus (S_1 \oplus S_4)(S_2 \oplus S_3)S_5 \\
f_2 &= S_1S_2 \oplus S_3S_4 \oplus S_5 \\
f_3 &= S_1S_2 \oplus S_3S_4 \oplus S_5S_6 \oplus S_7 \\
f_4 &= S_1\overline{S_4} \oplus S_2\overline{S_5} \oplus S_3\overline{S_6} \oplus S_1S_2S_3
\end{aligned}
$$

voorbeeld cryptoanalyse in syllabus

ExlusiveOr-som

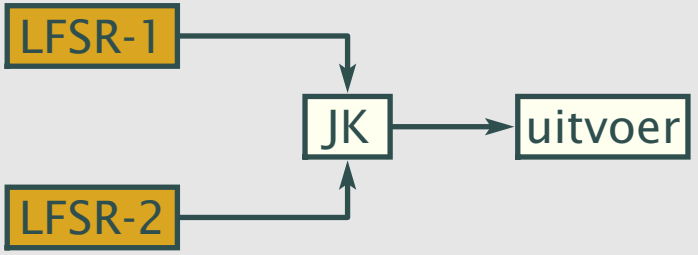


S_1	S_2		s_t
0	0	→	0
0	1	→	1
1	0	→	1
1	1	→	0

- $LSFR_1 \oplus LSFR_2 = \frac{1}{f(x)} + \frac{1}{g(x)} = \frac{f(x)+g(x)}{f(x)g(x)}$
- effectief productregister $f(x)g(x)$
- lineair equivalent $n_f + n_g$, periode $kgv((2^{n_f}-1),(2^{n_g}-1))$
- geen niet-lineariteit want $\oplus$ is lineaire operator
- AND en OR ook ongeschikt want driekwart 0'en resp. 1'en

JK–flipflop

$$f(S) = S_1 + (\overline{S_1 + S_2})s_{i-1}$$



S_1	S_2		s_t
0	0	→	s_{t-1}
0	1	→	0
1	0	→	1
1	1	→	$\overline{s_{t-1}}$

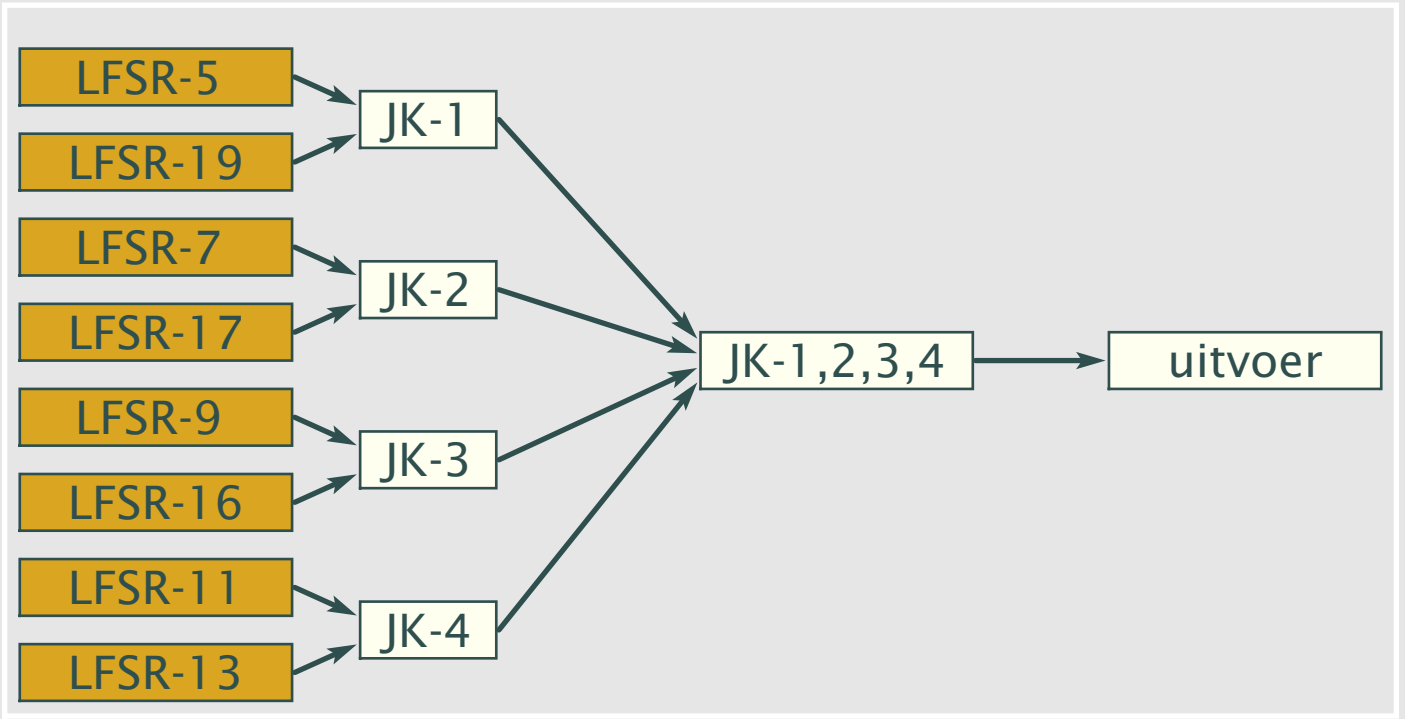
$$s(t-1)s(t) \rightarrow s_1(t) \text{ of } s_2(t)$$

$s_1 =$??01???01????1?01??01?001

$s =$ 100111001111010011001000 1 →

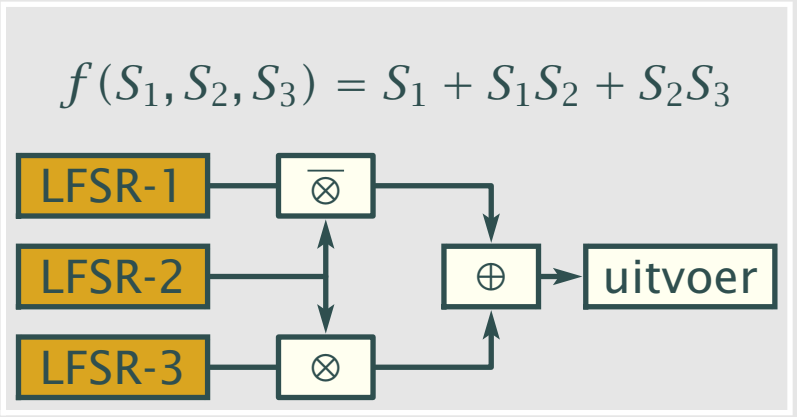
$s_2 =$?1??001??0001?1??01??1???

Pless-generator



LFSR-combinatie

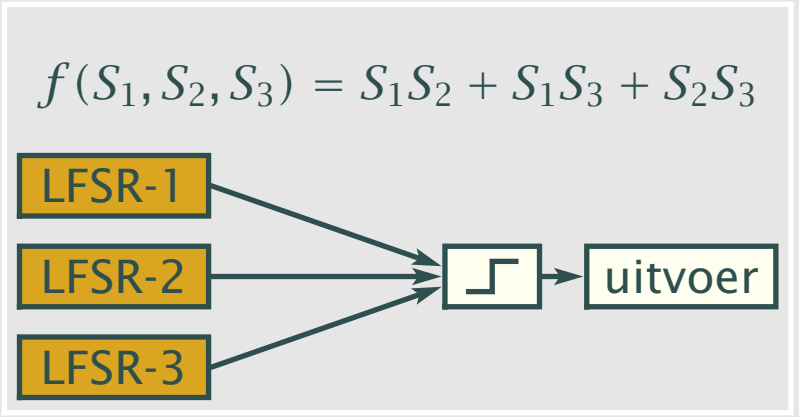
Geffe-generator



S_1	S_2	S_3		s_t
0	0	0	→	0
0	0	1	→	0
0	1	0	→	0
0	1	1	→	1
1	0	0	→	1
1	0	1	→	1
1	1	0	→	0
1	1	1	→	1

- $p = kgv((2^{n_1} - 1), (2^{n_2} - 1), (2^{n_3} - 1))$
- $LC = n_1 + n_1n_2 + n_2n_3$
- correlatie $2/3$ tussen s_t en S_1 / S_3

Bruer-generator

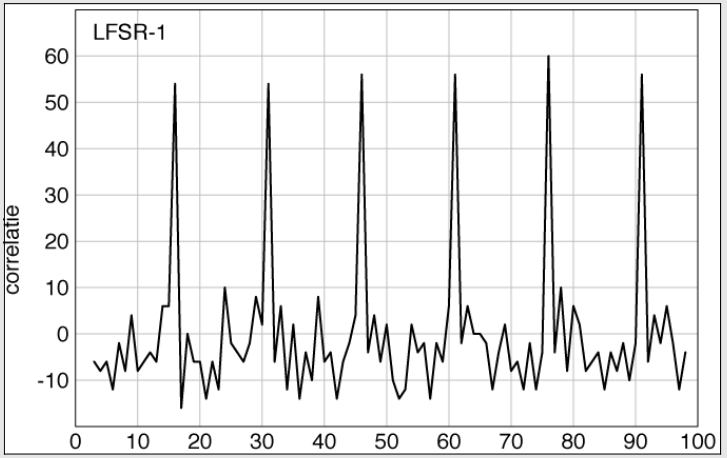


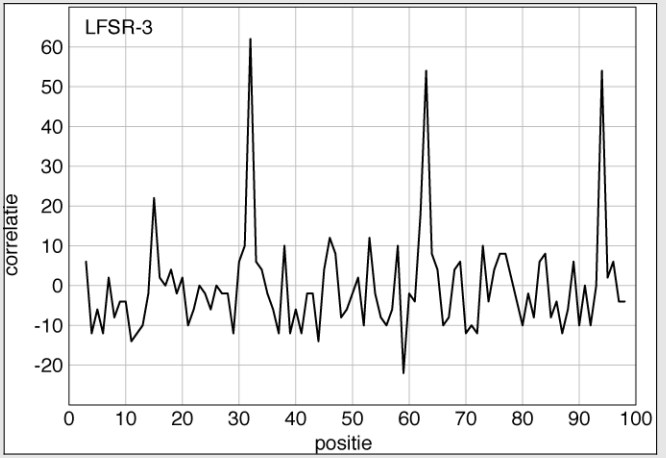
S_1	S_2	S_3		s_t
0	0	0	→	0
0	0	1	→	0
0	1	0	→	0
0	1	1	→	1
1	0	0	→	0
1	0	1	→	1
1	1	0	→	1
1	1	1	→	1

- $p = kgv((2^{n_1} - 1), (2^{n_2} - 1), (2^{n_3} - 1))$
- $LC = n_1n_2 + n_1n_3 + n_2n_3$
- correlatie $2/3$ tussen s_t en S_1 / S_2 / S_3

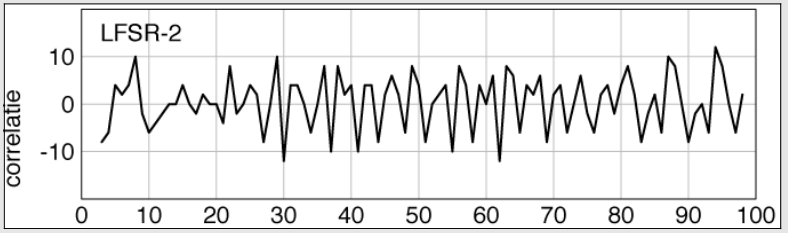
Siegenthaler *correlatie-aanval*

- voor *elke begintoestand* van $LFSR_i$ berekenen voor output s_t overeenstemming $s_t \oplus z_t$ met output van $F(LFSR_1, LFSR_2, \ldots)$
- correlatie $= \sum_{t=1}^{m} s_t \oplus z_t, \quad m \leq 2^n - 1$
- correlatie hoog als $\mid p(s_t = z_t) - 0.5 \mid > \epsilon$
- correlatie-immuniteit versus f in algebraïsche normaalvorm
- voorbeeld: Pless LFSR-19 nodig $\approx$ 350 bits
- voorbeeld: Geffe-generator met kleine LFSR's over 100 bits





Geffe generator



Correlatie-aanval

Correlatie-aanval op cijfertext

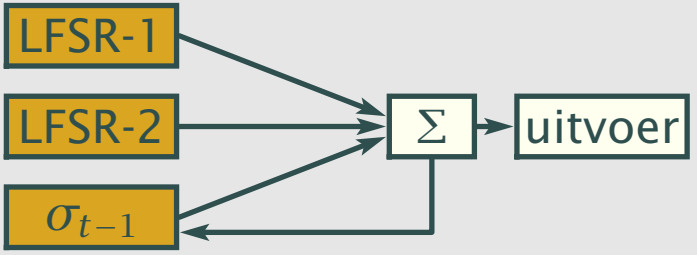
- effect minder geprononceerd tegen cijfertekst bits
- kans dat LFSR-bit s_i en cijfertekstbit c_i identiek zijn:
  $p = 1 - p_0 - q_{lfsr}(1 - 2p_0)$
  p_0 is kans op klaartekstbit = 0
  q_{lfsr} is correlatie tussen lfsr en generator
- p_0 kan per bit verschillen (bijv. hoogste bit in ASCII-byte)

- Meier-Staffelbach beperkt te onderzoeken begintoestanden
- voorbeeld $f(x) = 1 + x + x^{15} \rightarrow s_t = s_{t-14} + s_{t-15}$
  plus s_t in $S_0 \rightarrow s_{t+14} = s_t + s_{t-1}$ en s_t in $S_1 \rightarrow s_{t+15} = s_{t+1} + s_t$
- vervang s (output LFSR) door z (output generator)
  bereken kans dat vergelijkingen dan nog opgaan
  benader iteratief de reeks s_t uit de z_t's
- vergroot aantal vergelijkingen d.m.v. $f(x)^n$
  deze geven dezelfde uitvoer, met $n = 2^k$ niet meer taps
- effectiviteit neemt af met aantal taps in $f(x)$

Meier-Staffelbach aanval

Som-generator

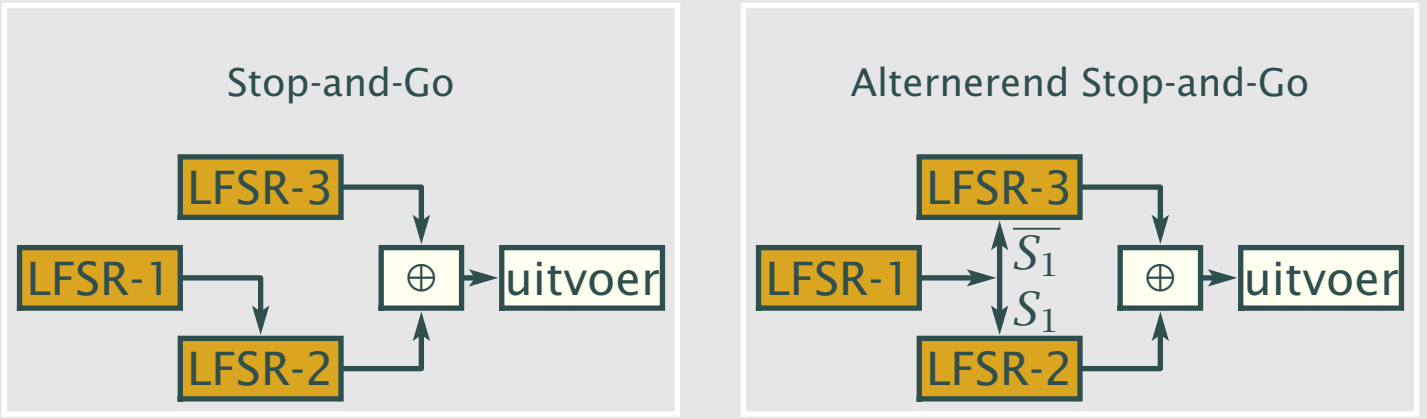
$$s_t = a_t \oplus b_t \oplus \sigma_{t-1}$$
$$\sigma_t = a_t b_t \oplus (a_t \oplus b_t)\sigma_{t-1}$$



S_1	S_2	σ_{t-1}		s_t	σ_t
0	0	0	→	0	0
0	0	1	→	1	0
0	1	0	→	1	0
0	1	1	→	0	1
1	0	0	→	1	0
1	0	1	→	0	1
1	1	0	→	0	1
1	1	1	→	1	1

- $p = (2^{n_1} - 1) \times (2^{n_2} - 1)$
- in eerste orde correlatie-immuun
- anticorrelatie 3/4 tussen s_t en σ_t

Stop–and–Go–generator



- $p = (2^{n_1} - 1) \times (2^{n_2} - 1) \times (2^{n_3} - 1)$
- $LC = (2^{n_1} - 1)n_2 + n_3$
- correlatie $s_t = s_{t+1} \rightarrow s_t \oplus s_{t+1} = S3_t \oplus S3_{t+1}$

$s_t = S_2(t)$ *iff* $S_1(t) = 1$
$S_1 = 1 + x^2$: 10110110110110110110
$S_2 = 1 + x + x^3$: 10010111001011001011
s_t : 1 01 11 00 01 10 10 1
$p = 2^{n_1-1}(2^{n_2}-1)$ $\quad 2^{n_1-2} < LC \leq n_2 2^{n_1-1}$

Krimpgenerator

$s_t = S(2t+1)$ *iff* $S(2t) = 1$
$S = 1 + x + x^3$: 10010111001011001011
s_t : 0 1 0 1 0
$p \geq 2^{n/2}$ $\quad LC > 2^{n/2-1}$

Zelfkrimpende generator

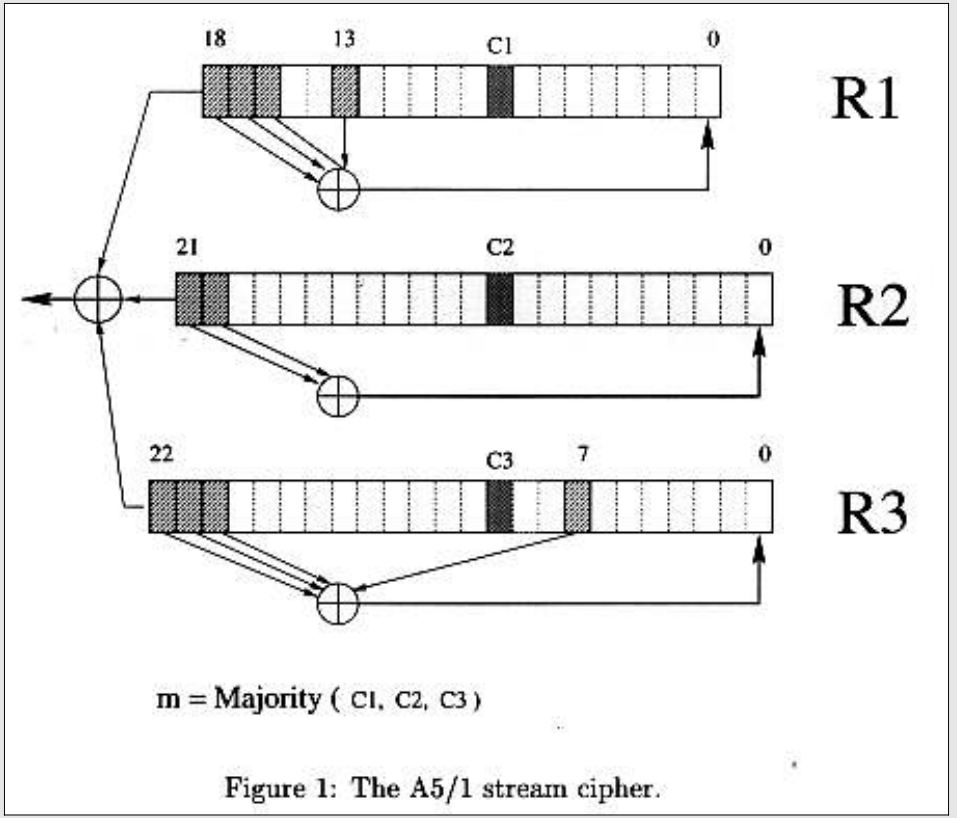


Figure 1: The A5/1 stream cipher.