Cursus Cryptografie

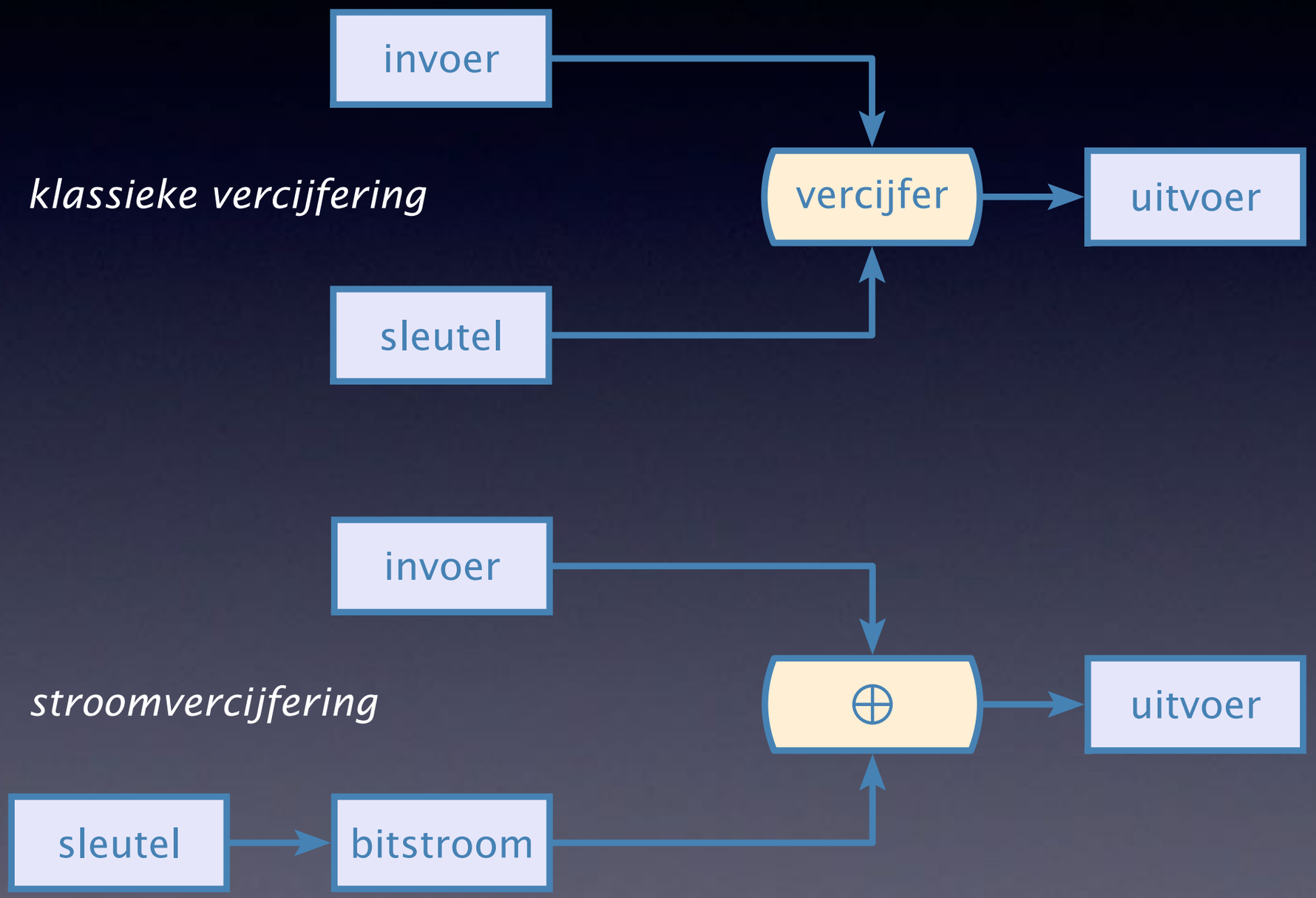
STROOMCIJFER

13-03-2017

Onderwerpen

- Principe
- Schuifregister
- Lineair schuifregister
- Periode en kwaliteit
- Niet-lineaire systemen
- Lineaire complexiteit
- Filtering
- LFSR-combinaties
- Correlatieaanval
- Kloksturing

Stroomvercijfering



klassieke vercijfering

stroomvercijfering

Vernam vercijfering

UPPER CASE	WEATHER SYMBOLS	↓	⊕	○	↙	3	→	↘	↓	8	↙	←	↖	•	●	9	ø	1	4	🔔	5	7	ⓣ	2	/	6	+	−	⟨	≡			
	COMMUNICATIONS	-	?	:	$	3	!	&	£	8	'	(	)	.	,	9	ø	1	4	🔔	5	7	;	2	/	6	"	≀	⟨	≡			
LOWER CASE		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	BLANK	C.R.	L.F.	SPACE	LTR. SHIFT	FIG. SHIFT
	1	●	●		●	●	●				●	●						●		●		●		●	●	●	●					●	●
	2	●		●				●		●	●	●	●				●	●	●			●	●	●						●		●	●
	3			●			●		●	●		●		●	●		●	●		●		●	●		●	●					●	●	
	4		●	●	●		●	●			●	●		●	●	●			●				●		●				●			●	●
	5		●					●	●				●	●		●	●	●			●		●	●	●	●	●					●	●

Baudot-code voor telex

Gilbert S. Vernam, 1917
telexcode + sleuteltape

WW-II Führer-Hauptkwartier ⇔ Wehrmacht-centra
Lorenz Schlüßelzusatz SZ40/42 (Bletchley Park 'Tunny')
Siemens Geheimschreiber T52-a/e (Zweden, Arne Beurling)

SZ42

T52

T52

Stroomvercijferen

vercijfering					
ASCII	H	a	l	l	o
klaar	01001000	01100001	01101100	01101100	01101111
sleutel	01100111	10101000	01000110	11010011	01000010
cijfer	00101111	11001001	00101010	10111111	00101101

ontcijfering					
cijfer	00101111	11001001	00101010	10111111	00101101
sleutel	01100111	10101000	01000110	11010011	01000010
klaar	01001000	01100001	01101100	01101100	01101111
ASCII	H	a	l	l	o

reconstructie sleutelstroom					
cijfer	00101111	11001001	00101010	10111111	00101101
klaar	01001000	01100001	01101100	01101100	01101111
sleutel	01100111	10101000	01000110	11010011	01000010

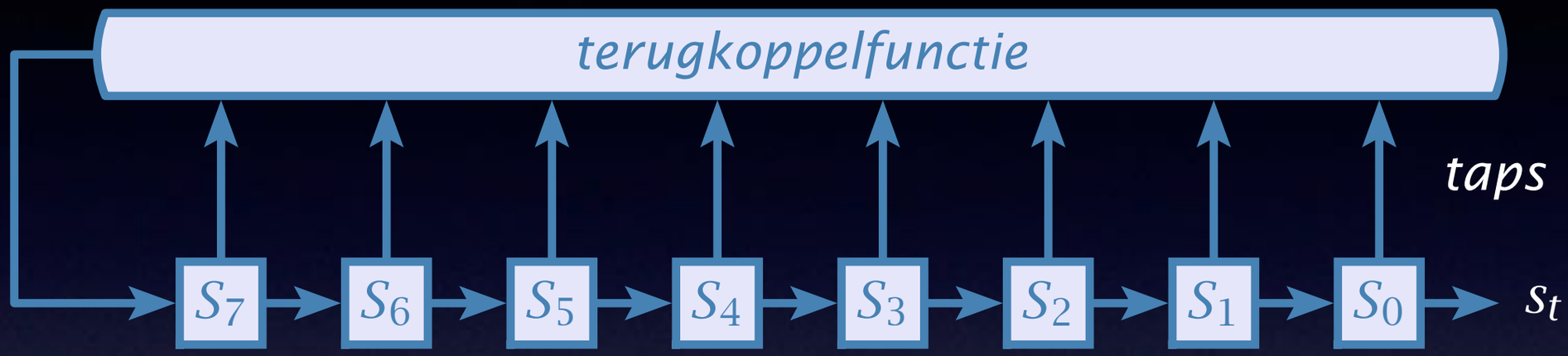
Kwaliteit

Golomb criteria (*Shift Register Sequences, 1967*)

- aantal 1'en en 0'en zo goed mogelijk gelijk
- run = rij gelijke bits || blok = rij 1'en || gat = rij 0'en
  evenveel blokken als gaten van elke lengte
  aantal gaten en blokken kleiner naarmate langer
- uitfase-autocorrelatie is een constante
  p is de periode
  δ is de verschuiving 0,1…p -1

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

Schuifregister



registertoestand is $S_7S_6S_5S_4S_3S_2S_1S_0$

opeenvolging $S_7S_6S_5S_4S_3S_2S_1S_0\,(t-1) \rightarrow S_7S_6S_5S_4S_3S_2S_1S_0\,(t)$

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

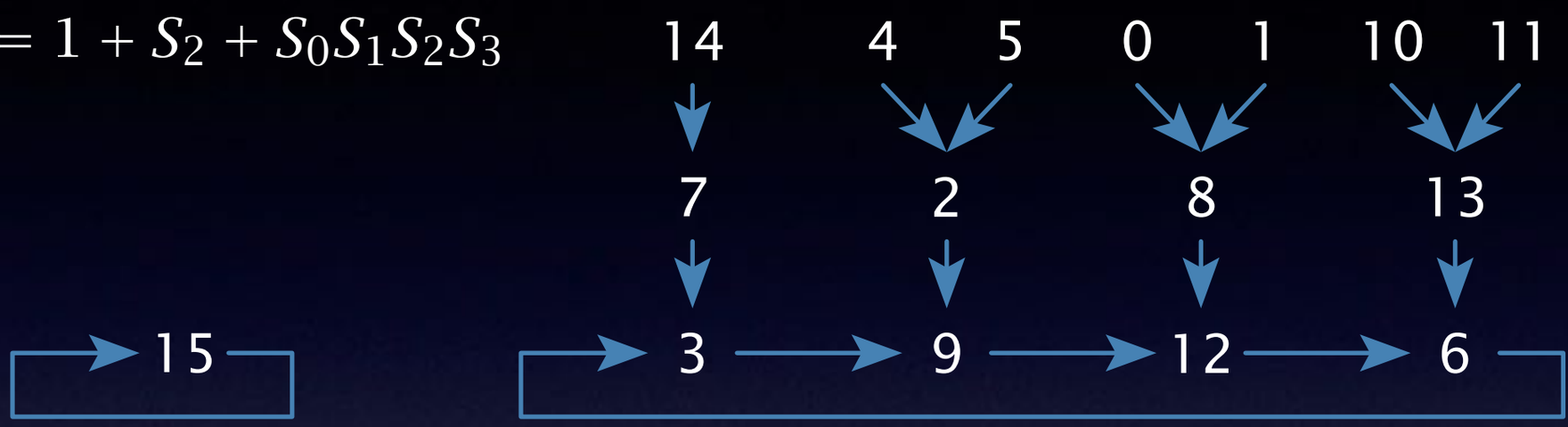
$s_t = S_0(t)$, $S_0(t) = S_1(t) \ldots S_7(t) = f(S_0 \ldots S_7)(t)$

Terugkoppelfunctie

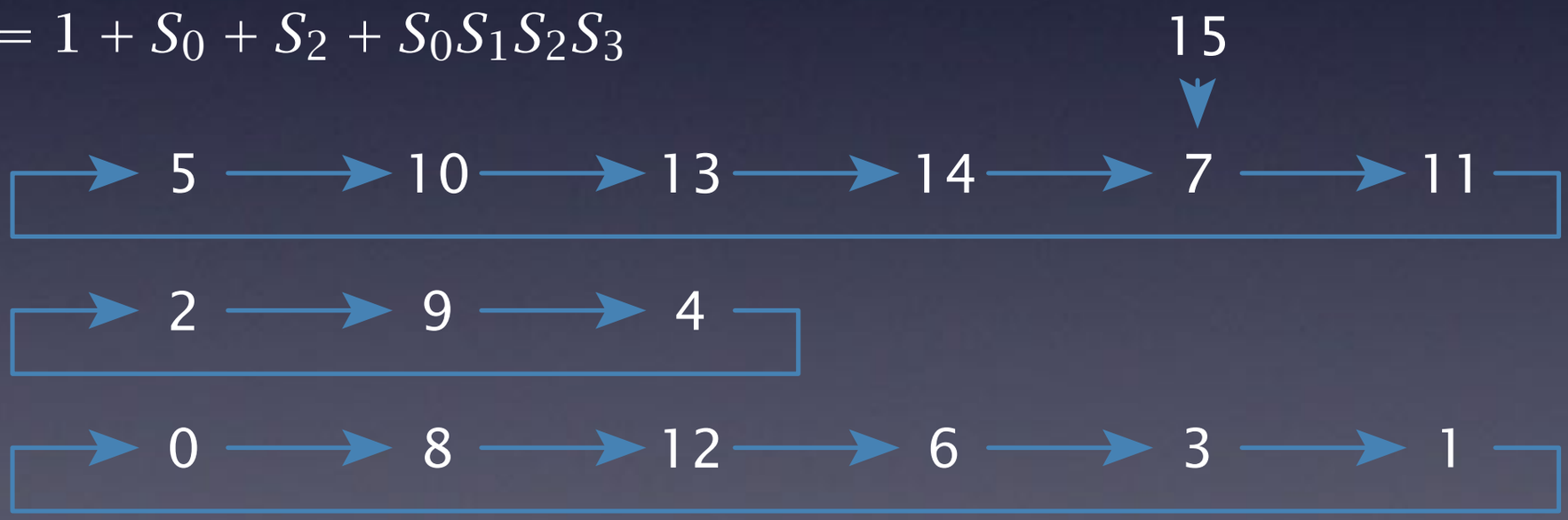
- voorbeeld f = 1 + S_0 + S_1S_3 +S_2S_4 + $S_1S_2S_3S_4$
- algebraïsche normaalvorm
  f = 1 + S_0 + ... + S_n + S_0S_1 + ... + $S_{n-2}S_{n-1}$ + $S_0 \ldots S_{n-1}$
- *n*-traps register heeft 2^{2^n} terugkoppelfuncties
- terugkoppelfunctie is te bepalen uit registertoestanden
- reeks opeenvolgende registertoestanden
  - losse cyclussen
  - vertakkingen
- maximale periode 2^n (De Bruin-rij, aantal $2^{2^{n-1}-n}$)

Voorbeelden

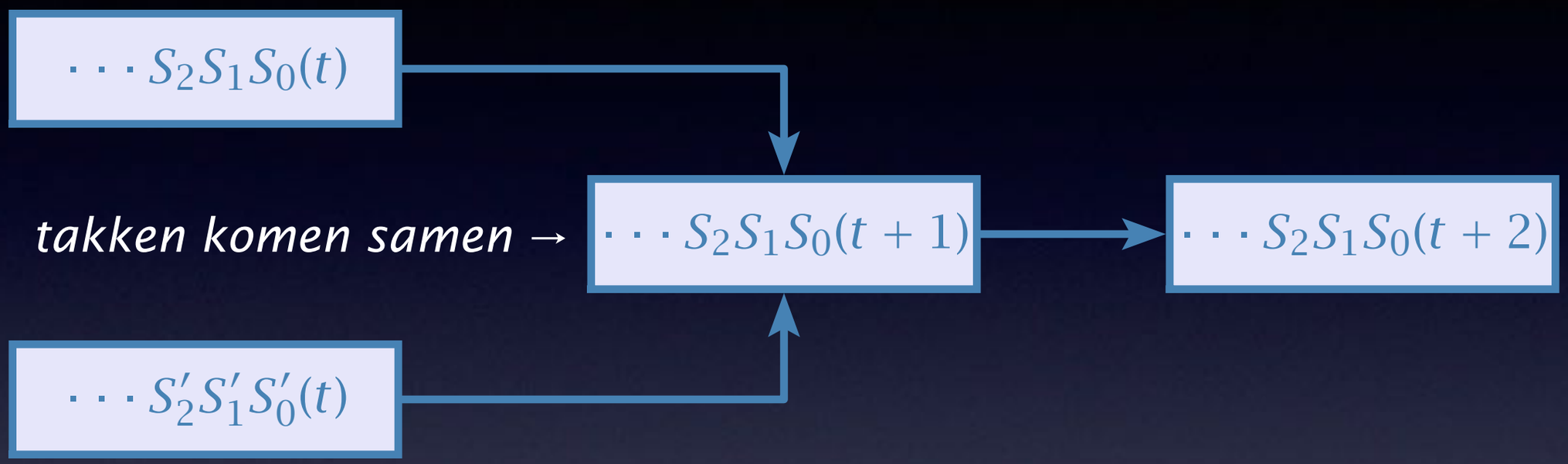
$f = 1 + S_2 + S_0S_1S_2S_3$



$f = 1 + S_0 + S_2 + S_0S_1S_2S_3$



Vertakkingspunten



Vlak voor samenkomst geldt

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

Vertakkingen ontbreken indien

$$f(S_0,S_1,S_2\ldots) = S_0 + f(S_1,S_2\ldots)$$

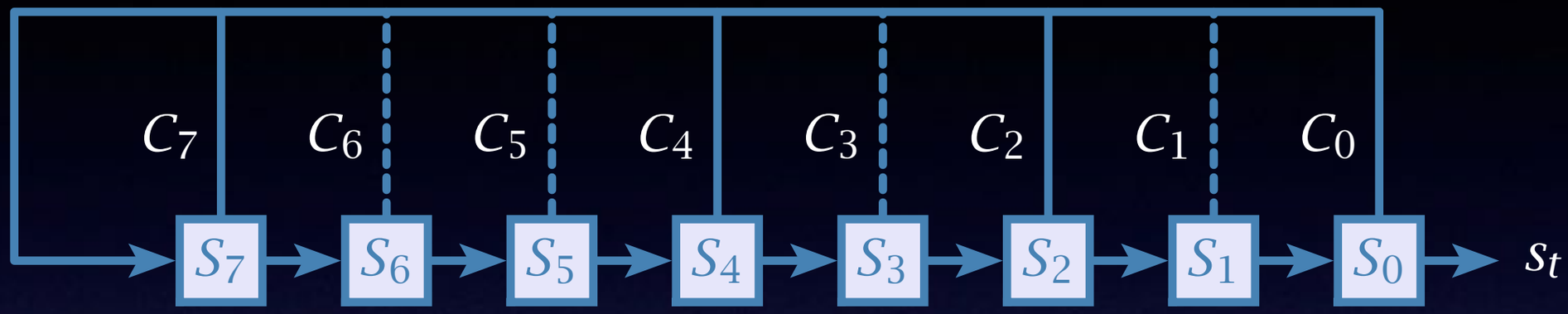
Functie berekenen

#	S_t	→	S_{t+1}	$f(S)$	selector voor S_t
0	0000		0000	0	$(S_3+1)(S_2+1)(S_1+1)(S_0+1)$
1	0001		1000	1	$(S_3+1)(S_2+1)(S_1+1)S_0$
2	0010		0001	0	$(S_3+1)(S_2+1)S_1(S_0+1)$
3	0011		0001	0	$(S_3+1)(S_2+1)S_1S_0$
4	0100		0010	0	$(S_3+1)S_2(S_1+1)(S_0+1)$
5	0101		0010	0	$(S_3+1)S_2(S_1+1)S_0$
6	0110		0011	0	$(S_3+1)S_2S_1(S_0+1)$
7	0111		1011	1	$(S_3+1)S_2S_1S_0$
8	1000		1100	1	$S_3(S_2+1)(S_1+1)(S_0+1)$
9	1001		0100	0	$S_3(S_2+1)(S_1+1)S_0$
10	1010		0101	0	$S_3(S_2+1)S_1(S_0+1)$
11	1011		0101	0	$S_3(S_2+1)S_1S_0$
12	1100		1110	1	$S_3S_2(S_1+1)(S_0+1)$
13	1101		1110	1	$S_3S_2(S_1+1)S_0$
14	1110		1111	1	$S_3S_2S_1(S_0+1)$
15	1111		0111	0	$S_3S_2S_1S_0$

$$f(S_0,S_1,S_2,S_3) = (S_3+1)(S_2+1)(S_1+1)S_0 + (S_3+1)S_2S_1S_0 + S_3(S_2+1)(S_1+1)(S_0+1) + S_3S_2(S_1+1)(S_0+1) + S_3S_2(S_1+1)S_0 + S_3S_2S_1(S_0+1)$$

$$= S_0 + S_3 + S_0S_1 + S_0S_2 + S_1S_3 + S_1S_2S_3$$

Lineair schuifregister



$$f(S) = C_0 S_0 \oplus C_1 S_1 \oplus \cdots \oplus C_{n-1} S_{n-1}$$

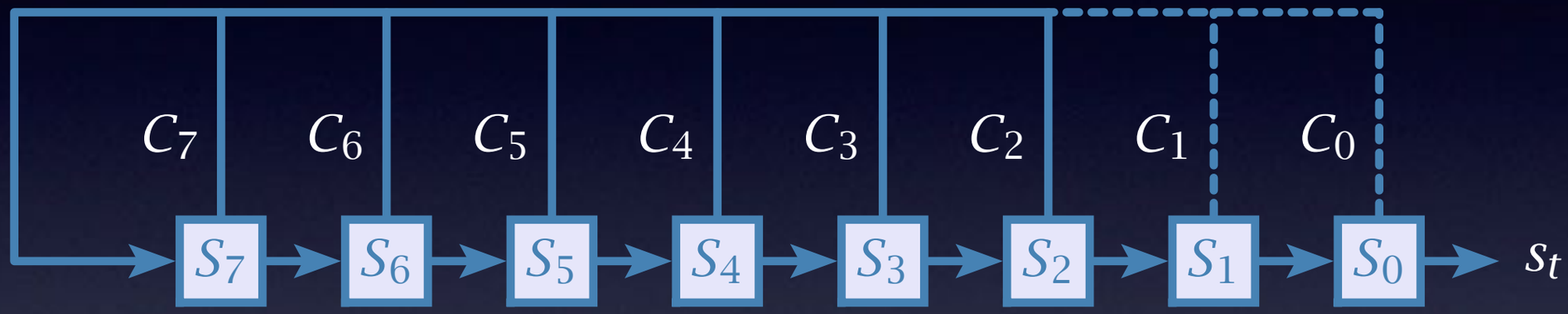
$$= \sum_{i=0}^{n-1} C_i S_i \qquad C_i \in \{0,1\}$$

$$\ldots s_t = C_{n-1} s_{t-1} \oplus \cdots \oplus C_0 s_{t-n}$$

$$= \sum_{i=1}^{n} C_{n-i} s_{t-i}$$

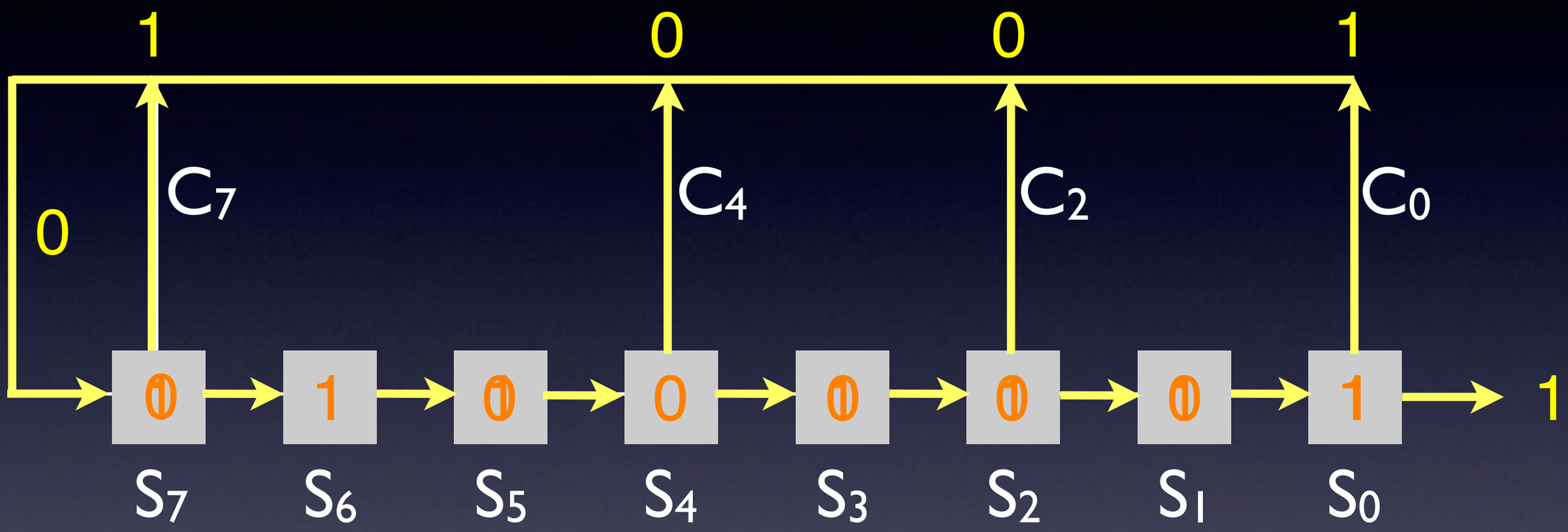
Terugkoppelfunctie

- omdat f = S_0 + S_1 +…+ S_{n-1} geen vertakkingen



- als $C_0 = C_1 = 0$ verkorting tot vertraagd 6-traps register dus als regel $C_0 = 1$
- Als $S_0 = S_1 = \ldots = S_{n-1} = 0$ dan $s_t = 0$ voor alle t
- er zijn daarom 2^n-1 registertoestanden ≠ 0…0
- dus maximaal mogelijke periode = 2^n-1 maximaalrij

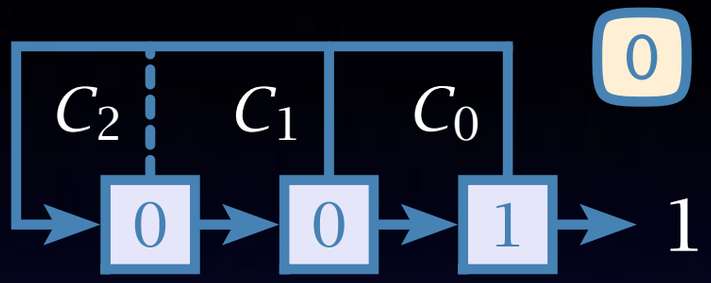
Werking LFSR

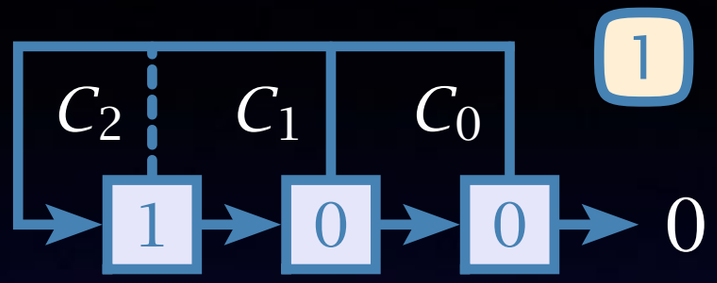


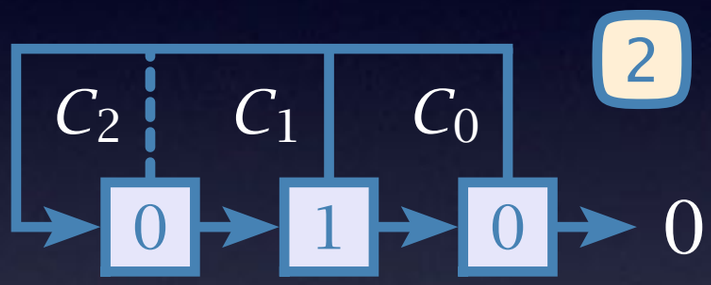
LFSR = Lineair Feedback Shift Register

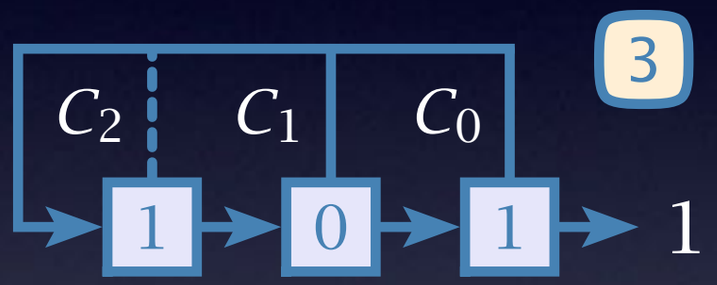
maximaalrij

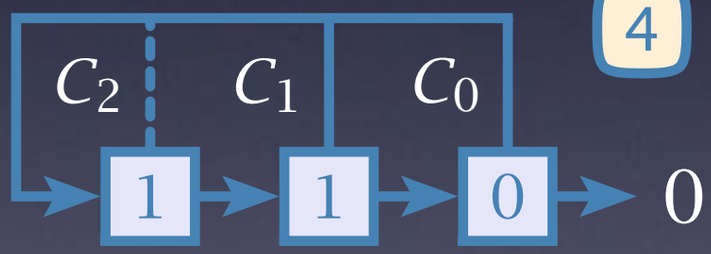
t	$S_2S_1S_0$	s_t
0	001	1
1	100	0
2	010	0
3	101	1
4	110	0
5	111	1
6	011	1
0	001	1
$p = 1001011$		
7	000	0
$p = 0$		

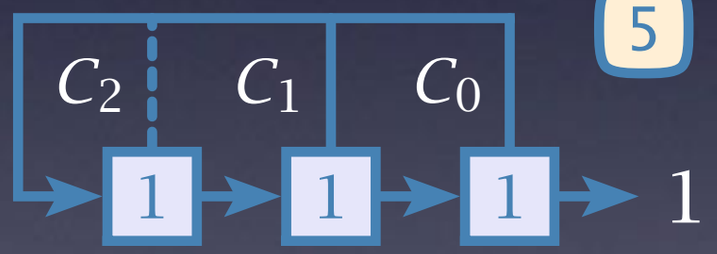


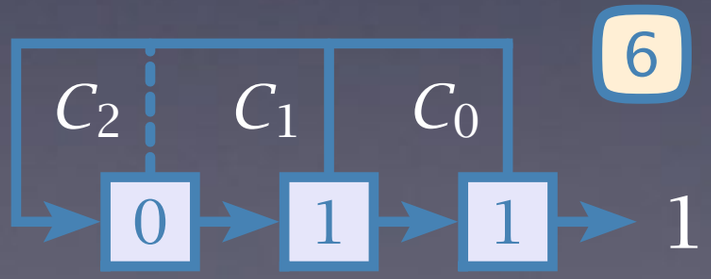


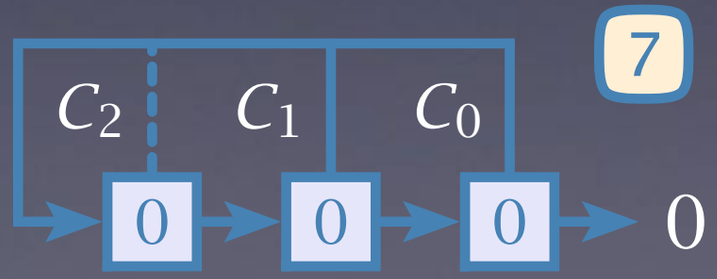






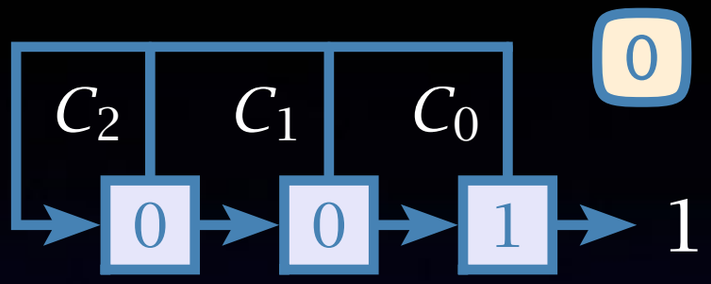


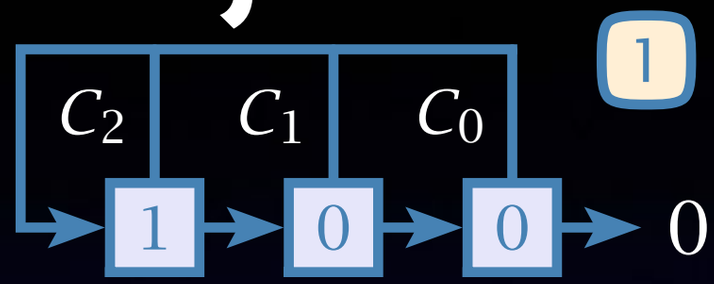


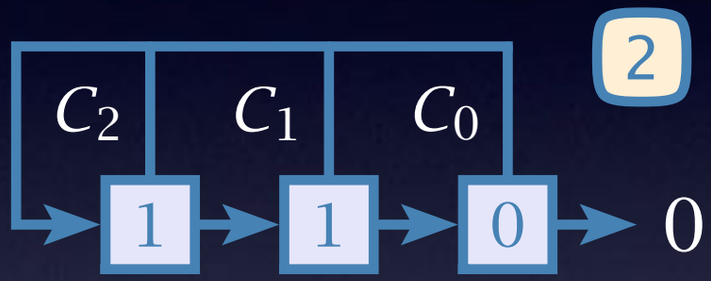


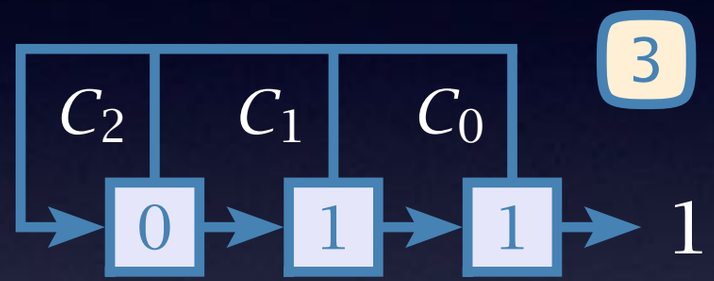
niet-maximaalrij

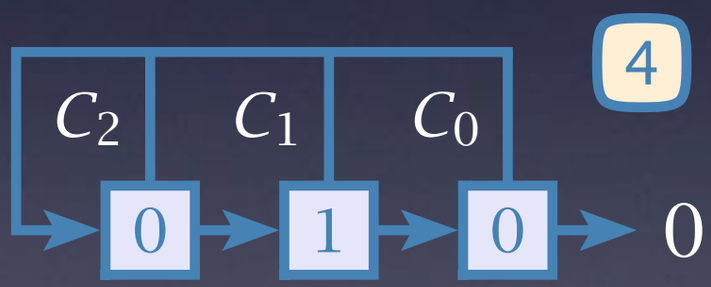
t	$S_2S_1S_0$	s_t
0	001	1
1	100	0
2	110	0
3	011	1
$p = 1001$		
4	010	0
5	101	1
$p = 01$		
6	111	1
$p = 1$		
7	000	0
$p = 0$		

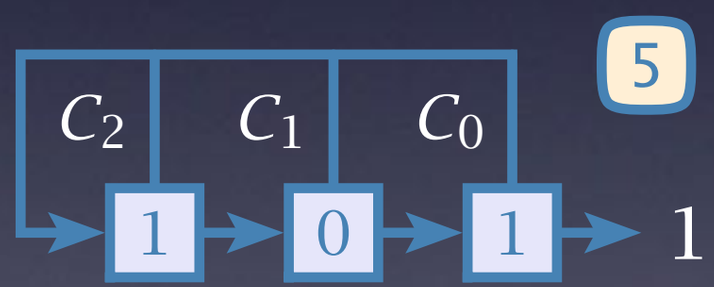


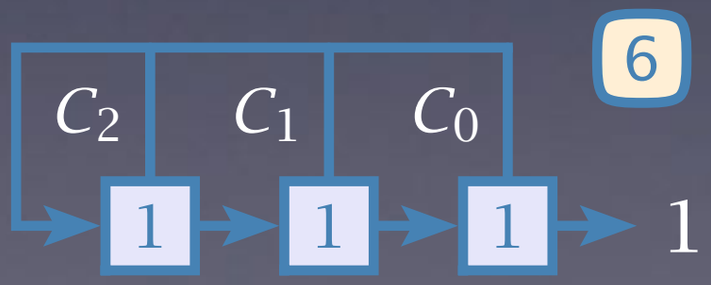


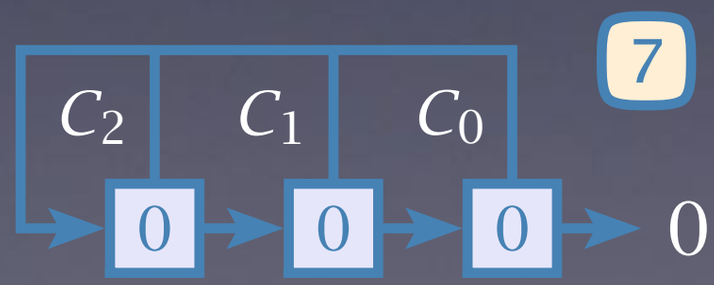




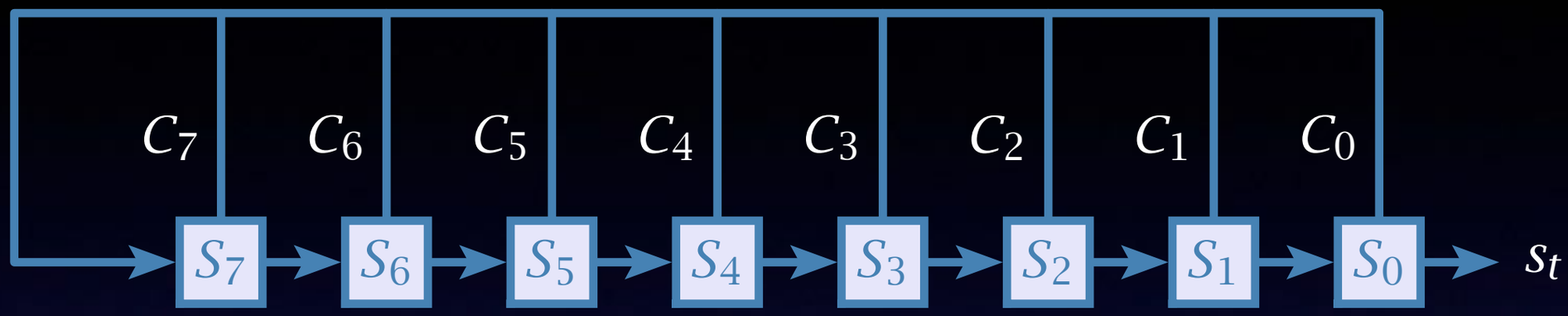




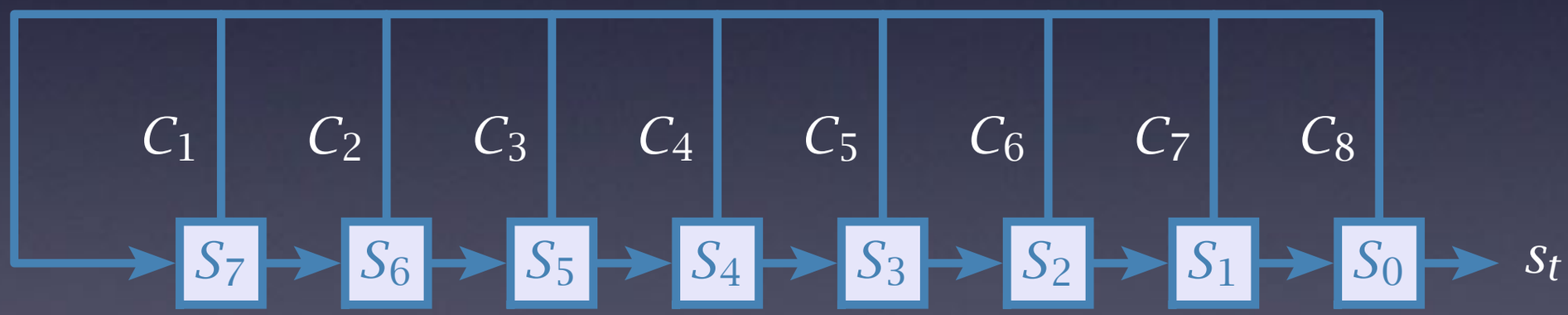




Alternatieve nummering



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



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

Periode LFSR

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

$$G(x) = \sum_{t=0}^{\infty} x^t \sum_{i=1}^{n} C_{n-i} s_{t-i}$$

$$= \sum_{i=1}^{n} C_{n-i}\, x^i \sum_{t=0}^{\infty} s_{t-i} x^{t-i}$$

$$= \sum_{i=1}^{n} C_{n-i}\, x^i \{s_{-i}x^{-i} + \cdots s_{-1}x^{-1} + \cdots + s_t x^t + \cdots\}$$

$$= \sum_{i=1}^{n} C_{n-i}\, x^i \{s_{-i}x^{-i} + \cdots s_{-1}x^{-1} + G(x)\}$$

$G(x)$ nu oplossen uit deze vergelijking

Periode LFSR

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

$$G(x) = \frac{s(x)}{f(x)} \quad \text{kies } S = 00\cdots01 \text{ dan } G(x) = \frac{1}{f(x)}$$

- teller hoogstens van graad n -1 en noemer van graad n
- teller representeert begintoestand van het register
- noemer onafhankelijk begintoestand = *karakteristieke functie*
- in alternatieve nummering karakteristieke functie is het *reciprook polynoom* $f^*(x) = x^n f(x^{-1})$

Periode LFSR

Verband leggen met de periode

$$G(x) = \sum_{t=0}^{\infty} s_t x^t = \sum_{k=0}^{\infty} \sum_{i=0}^{p-1} s_{i+k.p} x^{i+k.p}$$

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

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

$$G(x) = \frac{1}{f(x)} \rightarrow f(x)(s_0 + s_1 x + \cdots + s_{p-1} x^{p-1}) = 1 - x^p$$

periode is kleinste p *karakteristieke functie* $f(x)$ deler van $1 - x^p$

Periode LFSR maximaal

Maximaalrij *alleen als* karakteristieke functie $f(x)$ irreducibel

stel $f(x) = g(x)h(x)$ dan $\dfrac{1}{f(x)} = \dfrac{a(x)}{g(x)} + \dfrac{b(x)}{h(x)}$

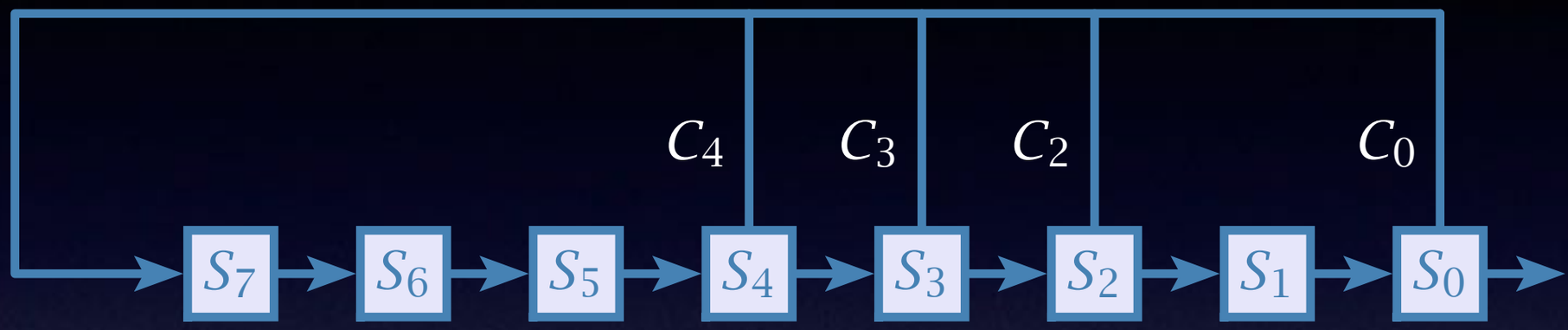
graad $n_f = n_g + n_h$

maximale periodes $p_f = 2^{n_f} - 1 \mid p_g = 2^{n_g} - 1 \mid p_h = 2^{n_h} - 1$

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

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

Karakteristieke functie



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

$$\text{aantal geschikte polynomen} = \frac{\phi(2^n - 1)}{n}$$

Golomb #1

- Golomb #1: *aantal enen en nullen zo gelijk mogelijk*
- kijk in maximaalrij naar het bit in S_0 elk bit komt erlangs
- er zijn in totaal 2^n bitcombinaties van n bits
- alle bitcombinaties behalve 00…00 worden doorlopen
- hiervan 2^{n-1} met bit 1 in S_0
- hiervan $2^{n-1}-1$ met bit 0 in S_0
- verschil 1 is best mogelijke bij oneven aantal
- conclusie LFSR voldoet aan Golomb #1

Golomb #2

- Golomb #2: *frequentie runs neemt af met hun lengte*
- blok van k 1'en betekent 01…10
- resteren n-k-2 bits dus 2^{n-k-2} blokken van lengte k
- idem 2^{n-k-2} gaten 10…01 van lengte k
- samen 2^{n-k-1} runs van lengte k
- bijtellen bijzondere gevallen 11…11 en 10…00
- totaal $2 + \sum_{k=1..n-2} 2^{n-k-1} = 2^{n-1}$ runs
- fractie runs van lengte k is $2^{n-k-1}/2^{n-1} = 1/2^k$
- conclusie LFSR voldoet aan Golomb #2

Golomb #3

- Golomb #3: *uitfase autocorrelatie is constant*
- uitfase autocorrelatie is

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

- combinatie van twee verschoven rijen is weer een andere rij uit de serie
- omdat $0 \oplus 0 = 1 \oplus 1 = 0$ en $0 \oplus 1 = 1 \oplus 0 = 1$ is aantal 0'en het aantal overeenkomstige in de combinatie
- resultaat voor autocorrelatie $-1/(2^n-1)$ is constant
- conclusie LFSR voldoet aan Golomb #3

LFSR cryptoanalyse

bereken s_t uit voorafgaande $s_{t-n} \cdots s_{t-1}$

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

met $2n$ opeenvolgende bits n lineaire vergelijkingen

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

oplossing $C_0 \ldots C_{n-1}$ → LFSR cryptografisch onveilig

Niet-lineaire systemen

- LFSR's worden benut als bouwstenen
- Lineaire complexiteit als maat
- Filtering
  - multiplex generator
  - filterfunctie
- Registercombinaties
  - Pless, Geffe, Bruer, som generator
  - correlatieaanval, correlatie-immuniteit
- Kloksturing
  - stop-and-go
  - krimpgenerator
  - A5/1 en A5/2 voor GSM

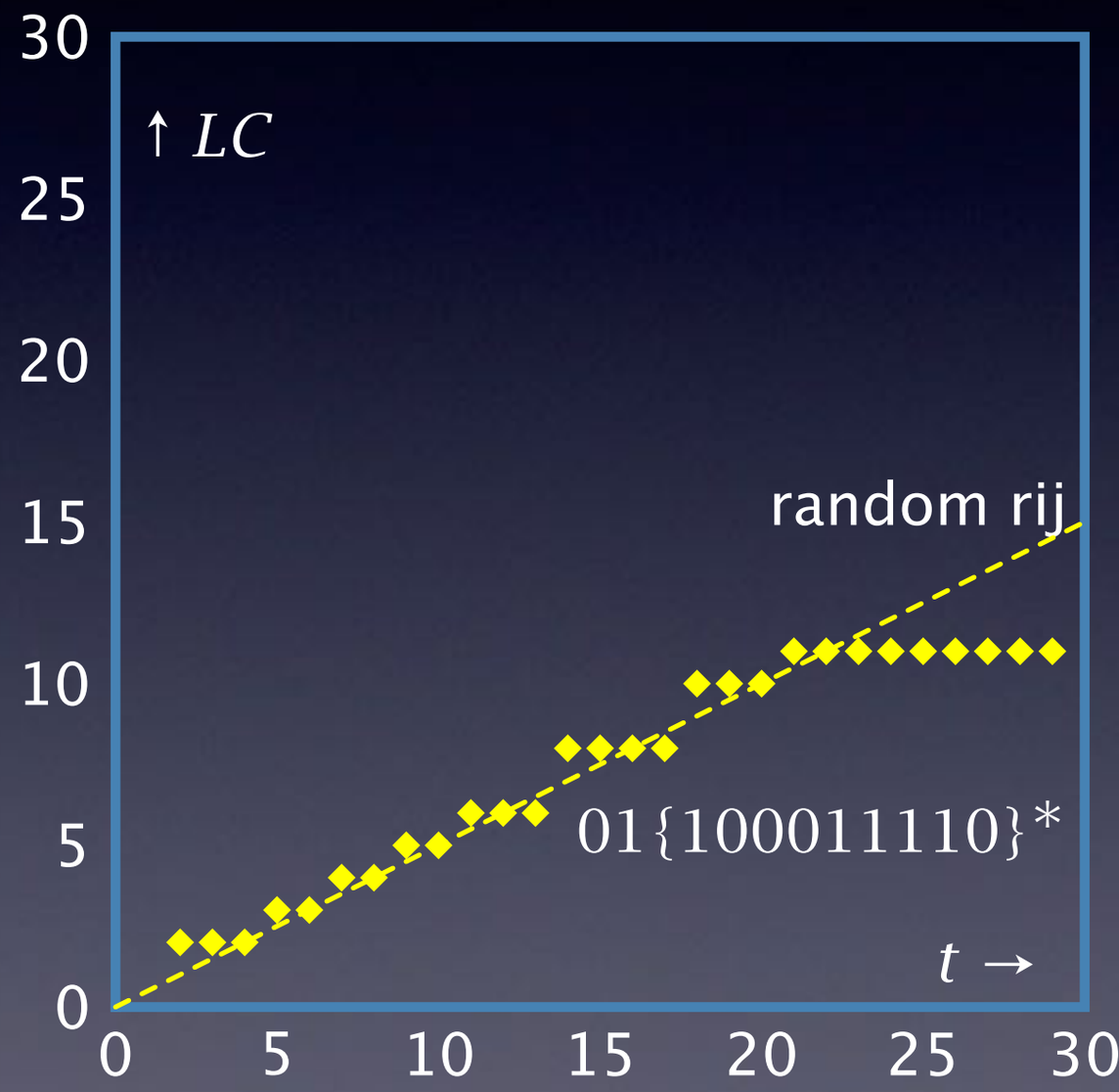
Lineaire complexiteit

- lineaire complexiteit is een equivalent LFSR
- Berlekamp-Massey algoritme
  - startregister reproduceert begin van bitrij
  - produceer bits zolang nieuw bit matcht
  - breidt register uit bij mismatch
- random bitrij van n bits lineaire complexiteit plm. n/2
- meer hogere termen in algebraïsche normaalvorm terugkoppelfunctie verhogen lineaire complexiteit

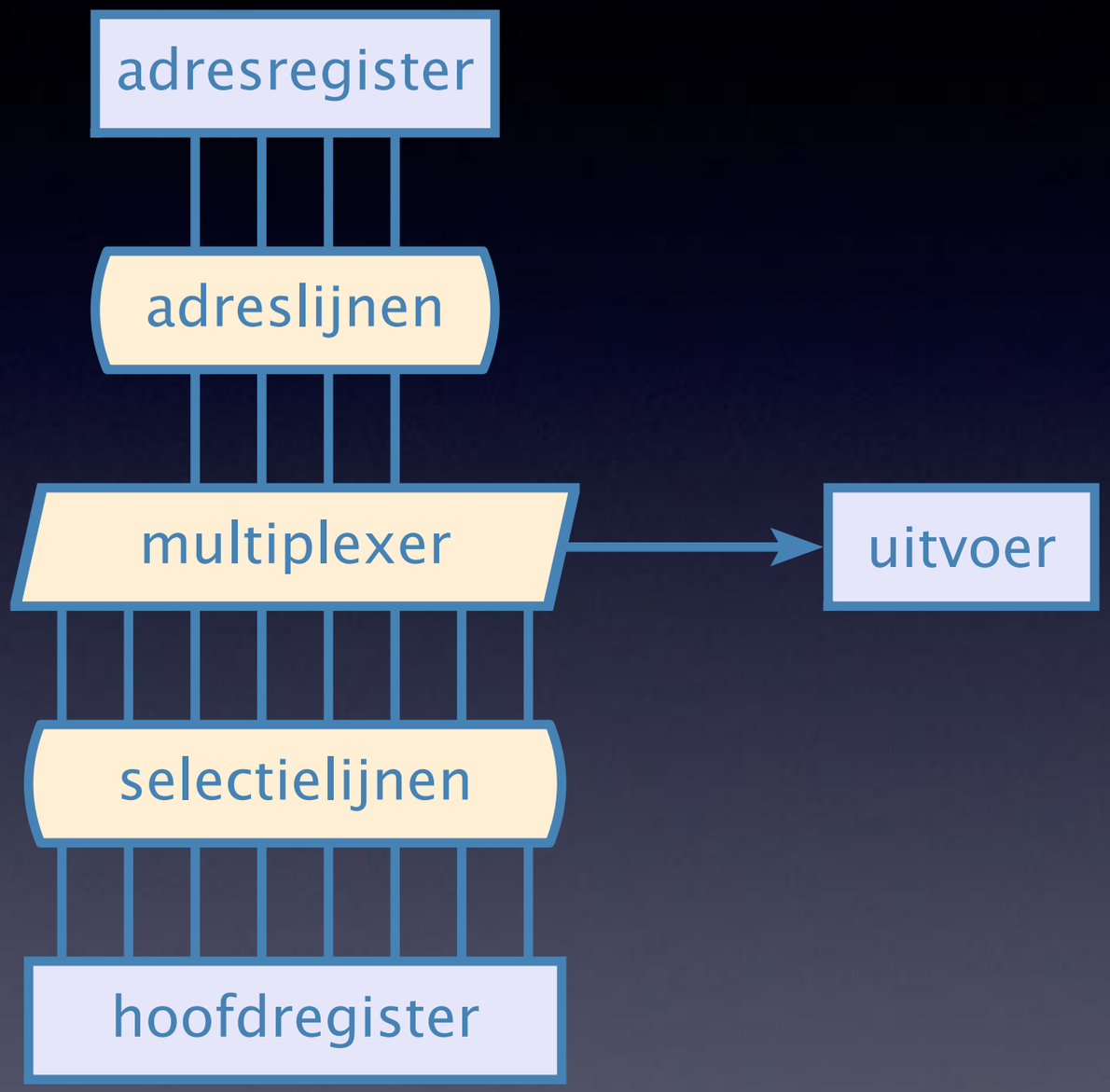
  S_1 en $S_1S_4S_7$ lage orde, $S_3S_4S_7S_9S_{12}S_{17}$ hoge orde

Voorbeeld complexiteit

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



Multiplexgenerator



voorbeeld cryptoanalyse zie syllabus

Filterfuncties

registertrappen uitgefilterd en gecombineerd

$$f_1 = S_1 \oplus S_2 \oplus (S_1 \oplus S_3)(S_2 \oplus S_4 \oplus S_5) \oplus (S_1 \oplus S_4)(S_2 \oplus S_3)S_5$$

$$f_2 = S_1S_2 \oplus S_3S_4 \oplus S_5$$

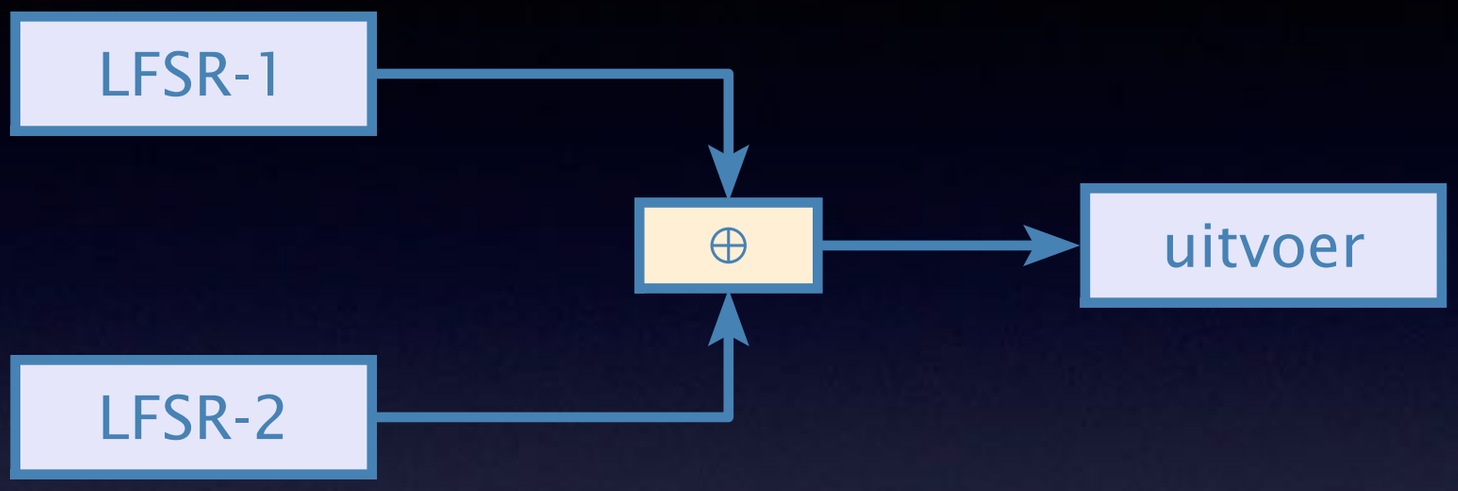
$$f_3 = S_1S_2 \oplus S_3S_4 \oplus S_5S_6 \oplus S_7$$

$$f_4 = S_1(1 + S_4) \oplus S_2(1 + S_5) \oplus S_3(1 + S_6) \oplus S_1S_2S_3$$

voorbeeld cryptoanalyse zie syllabus

Registercombinatie

$$f(S) = S_1 + S_2$$



S1	S2	f
0	0	0
0	1	1
1	0	1
1	1	0

$$LFSR_1 \oplus LFSR_2 = \frac{1}{f(x)} + \frac{1}{g(x)} = \frac{f(x) + g(x)}{f(x)g(x)}$$

effectief productregister $f(x)g(x)$

lineaire complexiteit $n_f + n_g$

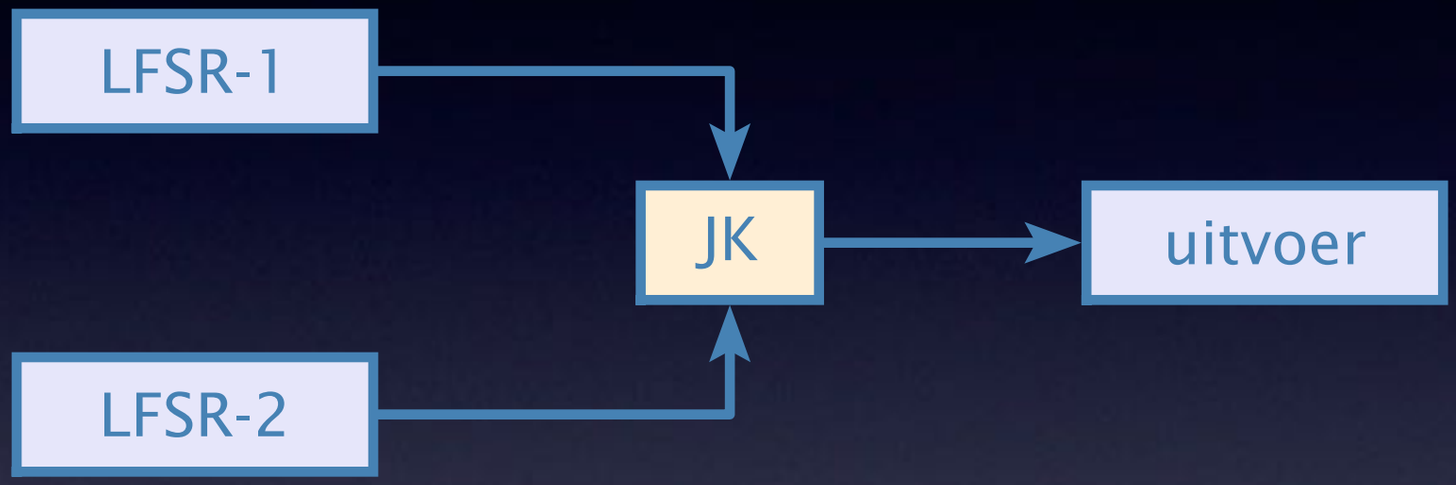
periode $\mathrm{kgv}((2^{n_f} - 1), (2^{n_g} - 1))$

geen niet-lineariteit want $\oplus$ is lineaire operator

and en or operatoren breken Golomb-1

JK-flipflop

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



S1	S2	f
0	0	S_{t-1}
0	1	0
1	0	1
1	1	$1+S_{t-1}$

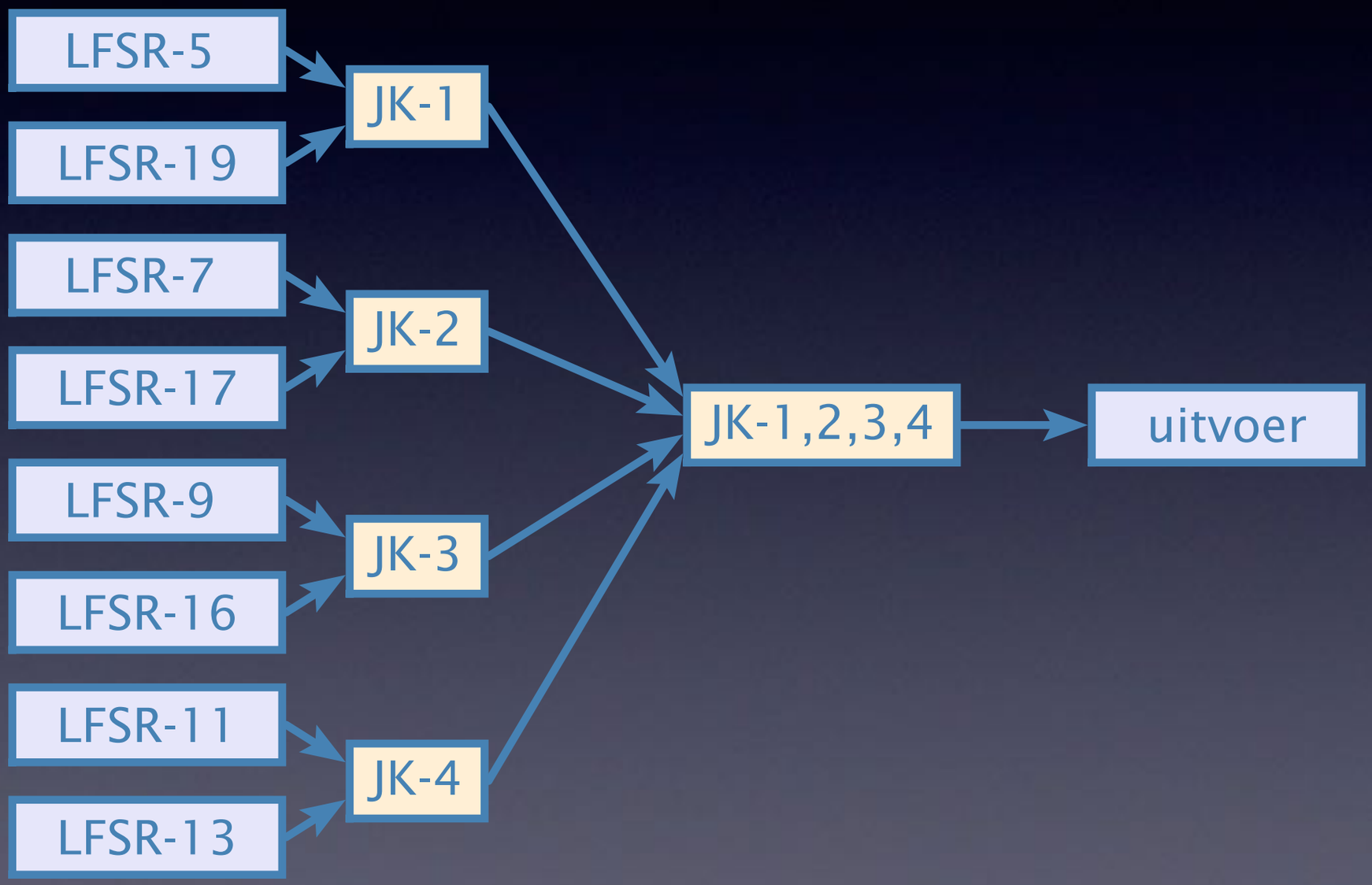
twee opeenvolgende bits → òf $s_1(t)$ òf $s_2(t)$

$$s = 10011100111101001100100001$$

$$\rightarrow s_1 = ??01???01????1?01??01?001$$

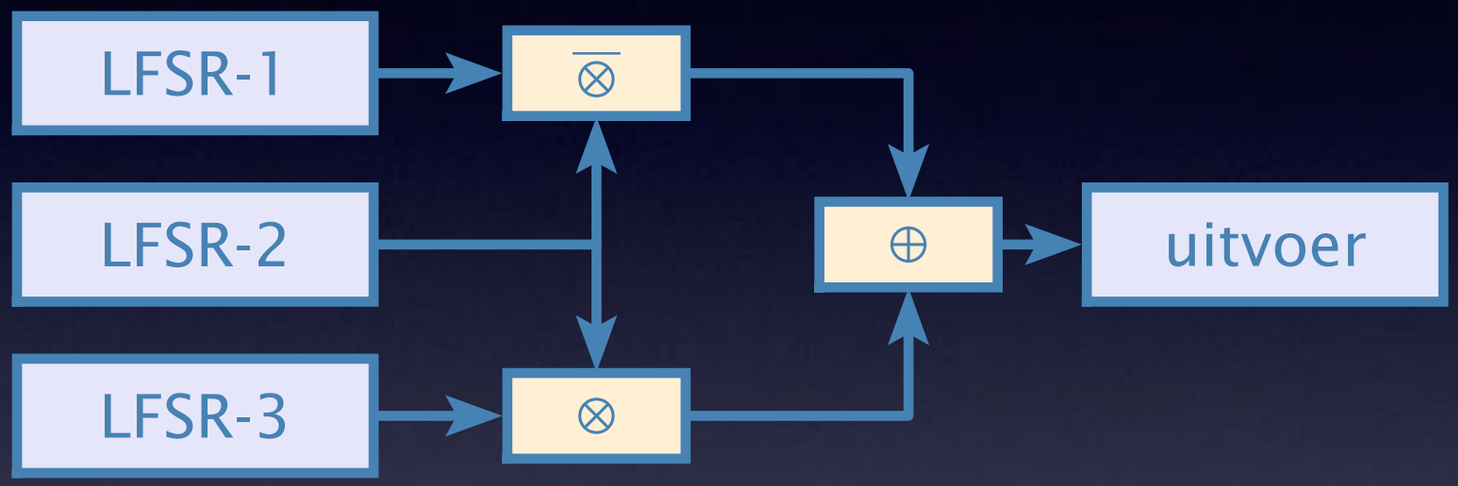
$$\rightarrow s_2 = ?1??001??0001?1??01??1???$$

Pless generator



Geffe-generator

$$f = S_1 + S_1S_2 + S_2S_3$$

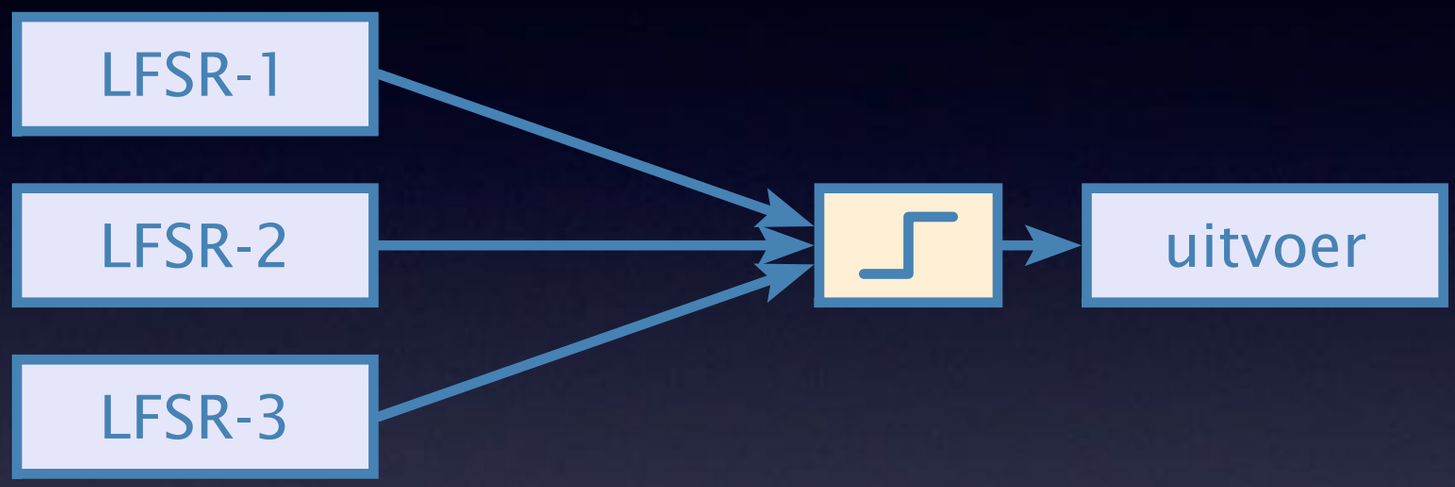


S1	S2	S3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

- periode is kgv van LFSR1, LFSR2, LFSR3
- lineaire complexiteit is $n_1 + n_1n_2 + n_2n_3$
- correlatie 75% tussen uitvoer en LFSR1/LFSR2

Bruer-generator

$$f = S_1S_2 + S_1S_3 + S_2S_3$$



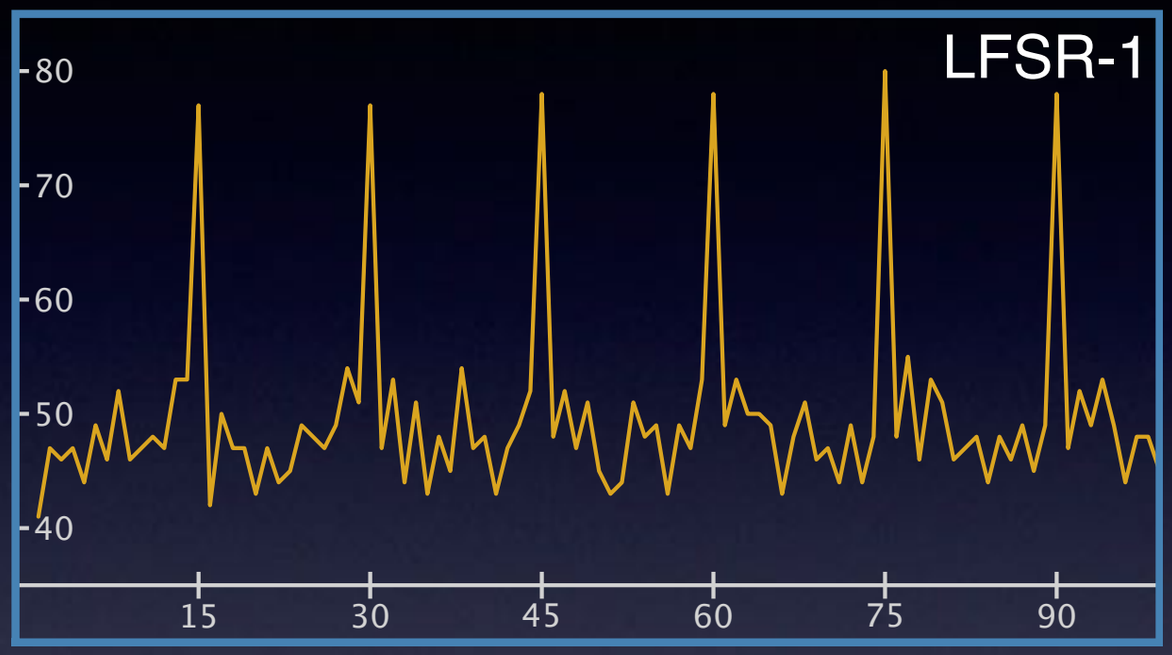
S1	S2	S3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

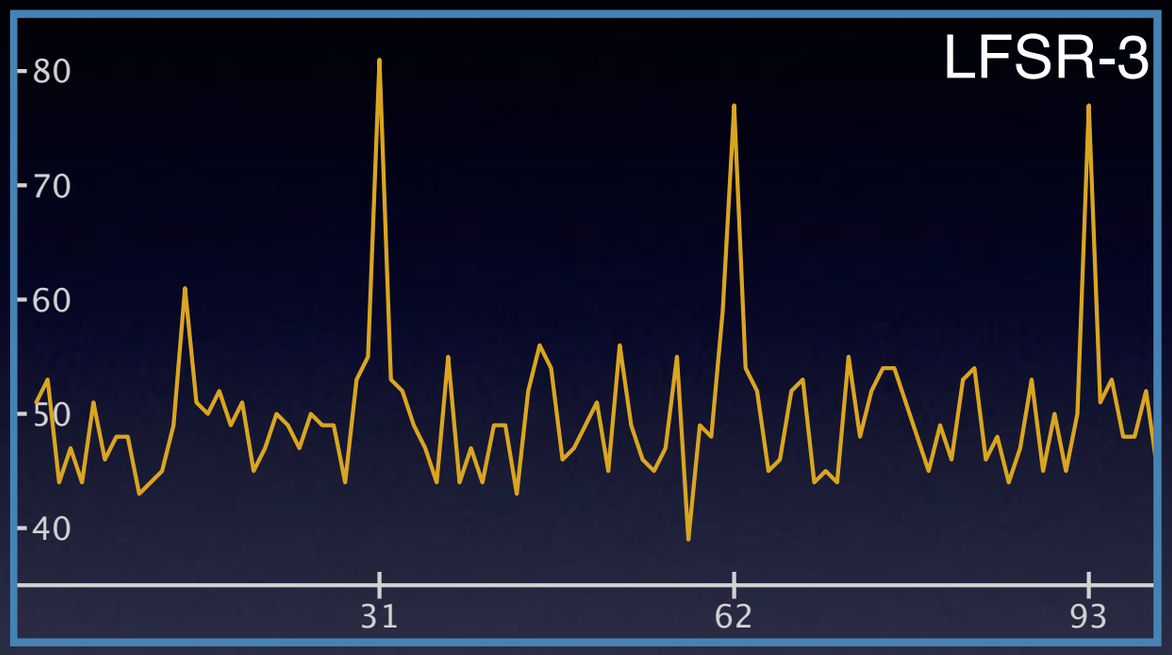
- periode is kgv van LFSR1, LFSR2, LFSR3
- lineaire complexiteit is $n_1n_2 + n_1n_3 + n_2n_3$
- correlatie 75% tussen uitvoer en LFSR1,LFSR2,LFSR3

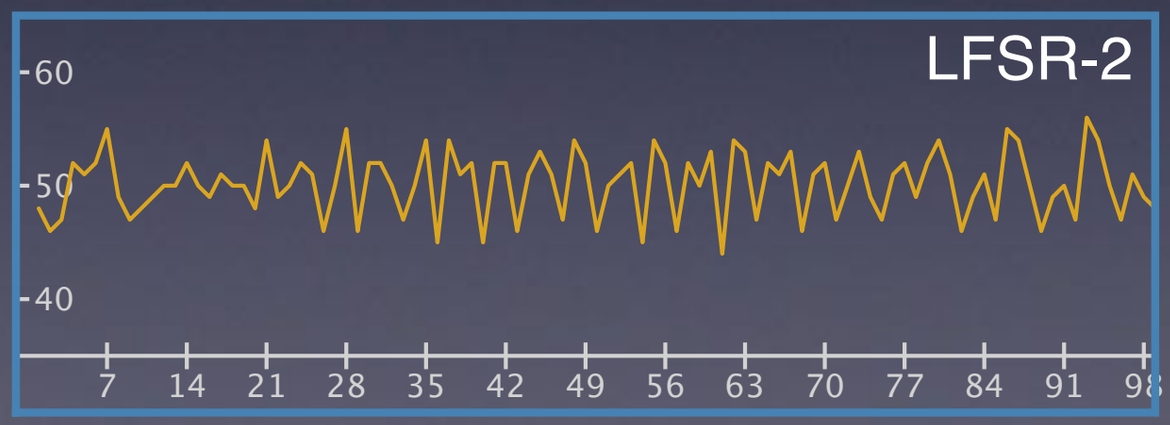
Siegenthaler-aanval

- voor elke begintoestand LFSRi output s vergelijken met output z van totale combinatie
- correlatie is $\sum_{t=1,m} s_t \oplus z_t$ voor $m \leq 2^n-1$
- correlatie hoog als kans $s_t=z_t$ afwijkt van 50%
- correlatie-immuniteit slechter met meer hogere termen in algebraïsche normaalvorm
- Pless-generator LSFR19 vergt ± 350 bits
- als voorbeeld Geffe-generator met kleine LFSR's en correlatiesom over 100 bits

Correlatie-aanval op Geffe







Aanval op cijfertekst

- effect minder duidelijk dan bij sleutelstroom
- kans dat LFSR-bit en cijfertekstbit gelijk 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
  bijvoorbeeld hoogste ASCII-bit is meestal 0

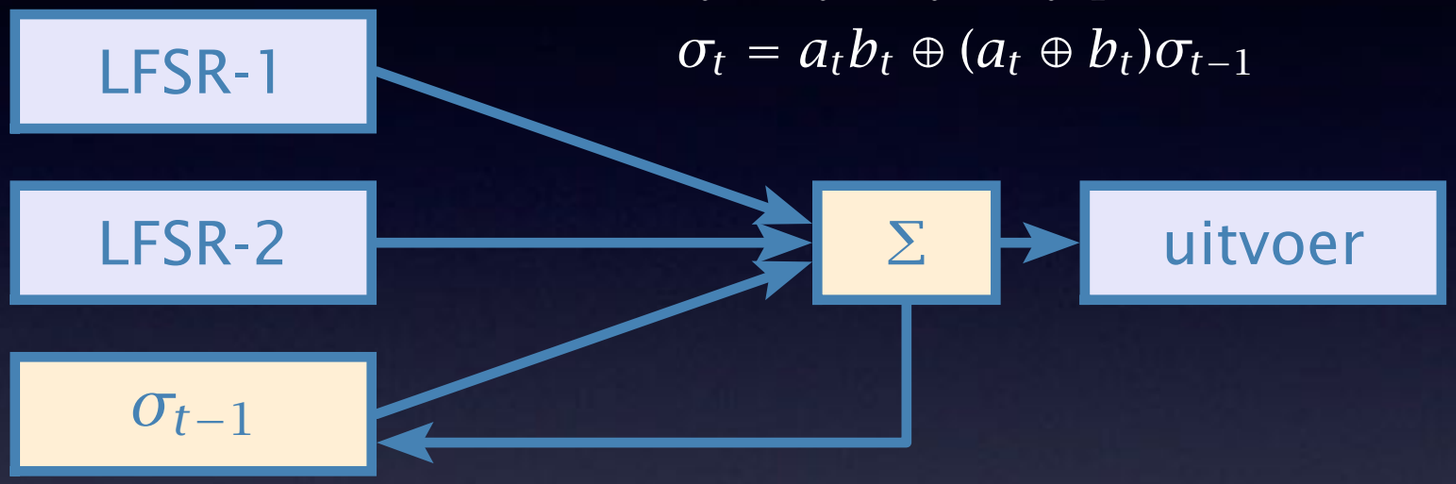
Meier-Staffelbach

- combineer meer outputbits in vergelijkingen
- voorbeeld $f(x) = 1 + x + x^{15}$
  (1) outputbit is $s_t = s_{t-14} + s_{t-15}$
  (2) bit in S_0 is $s_{t+14} = s_t + s_{t-1}$
  (3) bit in S_1 is $s_{t+15} = s_{t+1} + s_t$
- vervang s (output LFSR) door z (output generator)
  bereken kans dat vergelijkingen nog opgaan
  benader iteratief s_t uit z_t voor een reeks t
- vergroot aantal vergelijkingen met $f(x)^n$
  zelfde uitvoer zelfde aantal taps als $n = 2^k$
- effectiviteit aanval neemt af als meer taps in f(x)

Mastersectie

Somgenerator

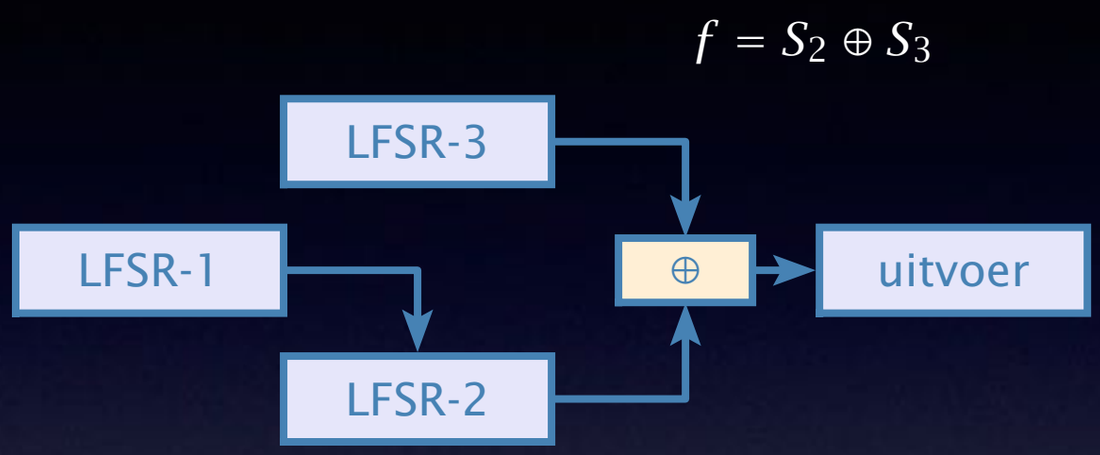
$$s_t = a_t \oplus b_t \oplus \sigma_{t-1}$$
$$\sigma_t = a_t b_t \oplus (a_t \oplus b_t)\sigma_{t-1}$$

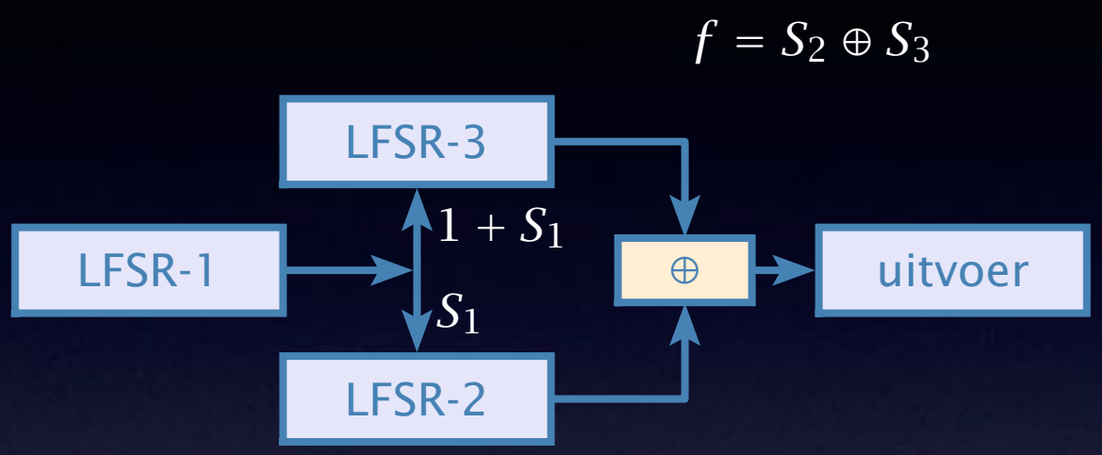


S1	S2	σ	f	σ
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

- periode is LFSR1 x LFSR2
- in eerste orde correlatie-immuun
- anticorrelatie 75% tussen uitvoer en σ

Stop-and-go





stop-and-go alternerend stop-and-go

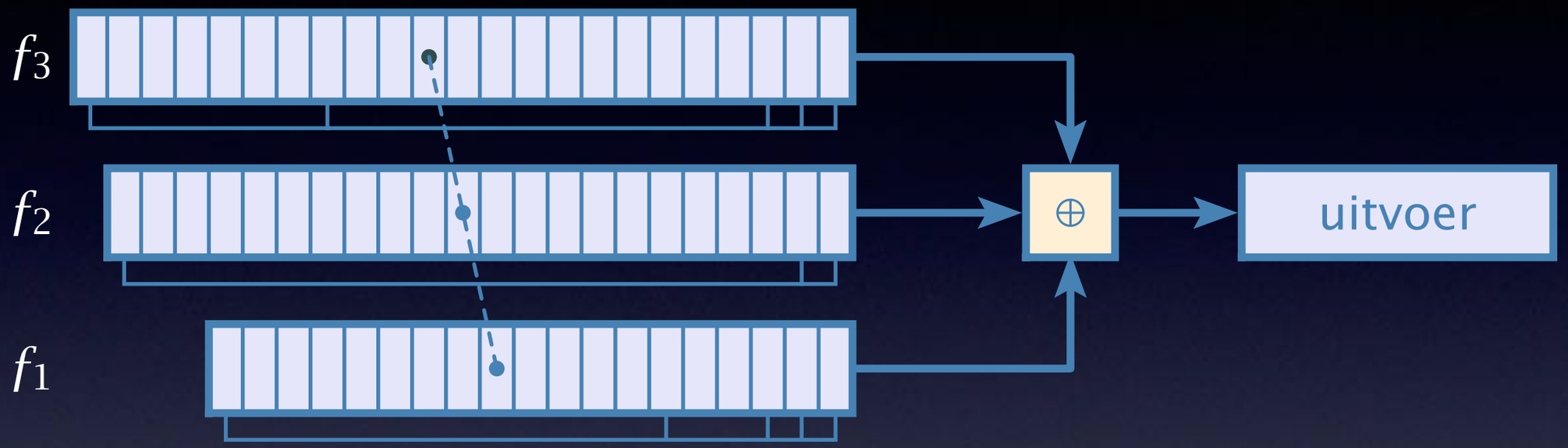
- periode is LFSR1 x LFSR2 x LFSR3
- lineaire complexiteit is $\text{periode}_{\text{LFSR1}}$ x n2 + n3
- correlatie tussen twee opeenvolgende bits en LFSR3

Krimpgenerator

krimpgenerator	
$s_t = S_2(t)$ indien $S_1(t) = 1$	
$S_1 = 1 + x^2$	10110110110110110110...
$S_2 = 1 + x + x^3$	10010111001011100101 1...
uitvoer	1 01 11 00 01 10 10 1...

zelfkrimpende generator	
$s_t = S(2t + 1)$ indien $S(2t) = 1$	
$S = 1 + x + x^3$	10010111001011100101 1...
uitvoer	0 1 0 1 0 ...

GSM-generator



$$f_1 = 1 + x + x^2 + x^5 + x^{19}$$
$$f_2 = 1 + x + x^{22}$$
$$f_3 = 1 + x + x^2 + x^{15} + x^{23}$$