Linear feedback shift registers

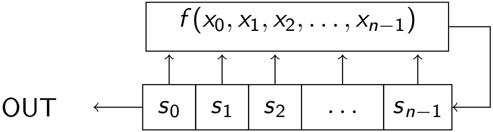
Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term.
$f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$

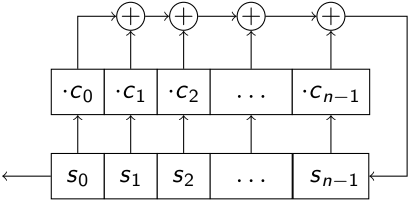


Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term. $f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$

Each state $S_j \in \mathbb{F}_2^n$, $S_j = (s_j \, s_{j+1} \, s_{j+2} \, \ldots \, s_{j+n-1})$. Coefficients $c_i \in \mathbb{F}_2$.

OUT



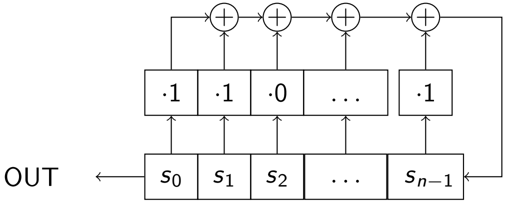
Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term.
$f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$

Each state $S_j \in \mathbb{F}_2^n$,
$S_j = (s_j\ s_{j+1}\ s_{j+2}\ \ldots\ s_{j+n-1})$.
Coefficients $c_i \in \mathbb{F}_2$.

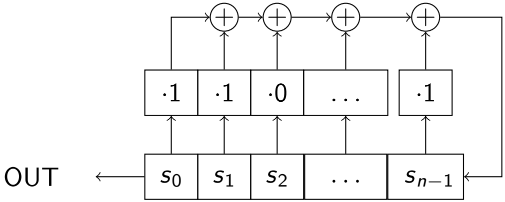
Typically $c_0 = 1$ (else we could have output one step earlier).

$IV = S_0$ Turn key k into
$k = c_0\, c_1\, c_2 \ldots c_{n-1}$



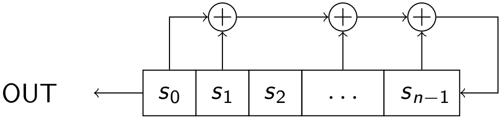
Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term.
$f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$



Each state $S_j \in \mathbb{F}_2^n$,
$S_j = (s_j\, s_{j+1}\, s_{j+2}\, \ldots\, s_{j+n-1})$.
Coefficients $c_i \in \mathbb{F}_2$.

Typically $c_0 = 1$ (else we could have output one step earlier).

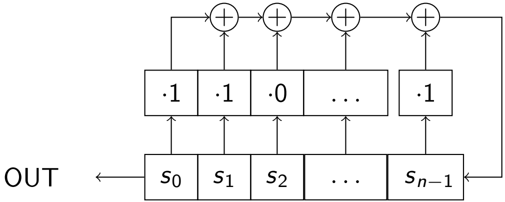


$IV = S_0$ Turn key k into
$k = c_0\, c_1\, c_2 \ldots c_{n-1}$

Simplify by putting connections for $c_i = 1$, no connections for $c_i = 0$.

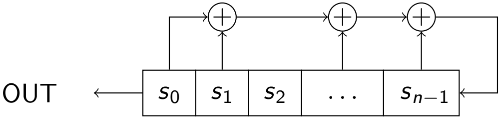
Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term.
$f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$



Each state $S_j \in \mathbb{F}_2^n$,
$S_j = (s_j \, s_{j+1} \, s_{j+2} \, \ldots \, s_{j+n-1})$.
Coefficients $c_i \in \mathbb{F}_2$.

Typically $c_0 = 1$ (else we could have output one step earlier).



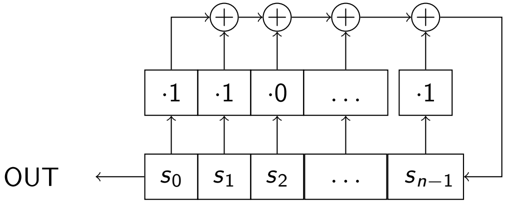
$IV = S_0$ Turn key k into $k = c_0 \, c_1 \, c_2 \ldots c_{n-1}$

Simplify by putting connections for $c_i = 1$, no connections for $c_i = 0$.

$f(x_0, x_1, x_2) = x_0 + x_2 =$

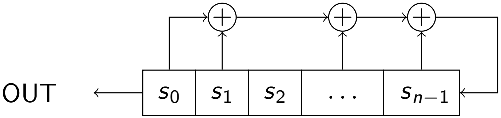
Linear feedback shift registers

Linear means that there are no products $x_i \cdot x_j$ and no constant term.
$f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$



Each state $S_j \in \mathbb{F}_2^n$,
$S_j = (s_j \; s_{j+1} \; s_{j+2} \; \dots \; s_{j+n-1})$.
Coefficients $c_i \in \mathbb{F}_2$.

Typically $c_0 = 1$ (else we could have output one step earlier).



$IV = S_0$ Turn key k into
$k = c_0 \, c_1 \, c_2 \dots c_{n-1}$

Simplify by putting connections for $c_i = 1$, no connections for $c_i = 0$.

$f(x_0, x_1, x_2) = x_0 + x_2 = 1 \cdot x_0 + 0 \cdot x_1 + 1 \cdot x_2.$

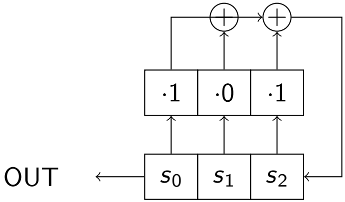
Linear feedback shift registers

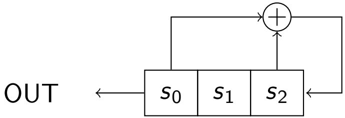
Linear means that there are no products $x_i \cdot x_j$ and no constant term. $f(\mathbf{x}) = \sum_{i=0}^{n-1} c_i x_i$

Each state $S_j \in \mathbb{F}_2^n$, $S_j = (s_j\, s_{j+1}\, s_{j+2}\, \ldots\, s_{j+n-1})$. Coefficients $c_i \in \mathbb{F}_2$.

Typically $c_0 = 1$ (else we could have output one step earlier).

$IV = S_0$ Turn key k into $k = c_0\, c_1\, c_2 \ldots c_{n-1}$



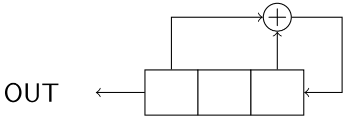


Simplify by putting connections for $c_i = 1$, no connections for $c_i = 0$.

$f(x_0, x_1, x_2) = x_0 + x_2 = 1 \cdot x_0 + 0 \cdot x_1 + 1 \cdot x_2$.

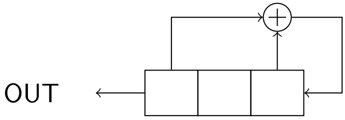
What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$



What is the period of $s_{j+3} = s_j + s_{j+2}$?

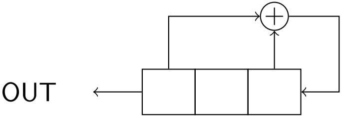
Starting state $S_0 = (0\ 0\ 1)$



0 0 1 1

What is the period of $s_{j+3} = s_j + s_{j+2}$?

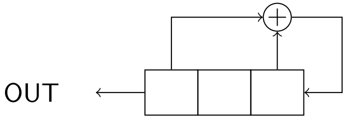
Starting state $S_0 = (0\ 0\ 1)$



	0	0	1	1
0	0	1	1	1

What is the period of $s_{j+3} = s_j + s_{j+2}$?

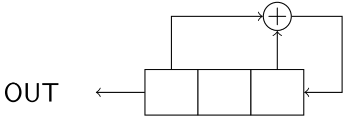
Starting state $S_0 = (0\ 0\ 1)$



	0	0	1	1
0	0	1	1	1
0	1	1	1	0

What is the period of $s_{j+3} = s_j + s_{j+2}$?

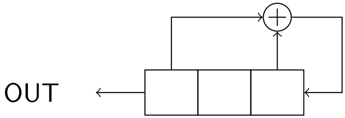
Starting state $S_0 = (0\ 0\ 1)$



	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1

What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$

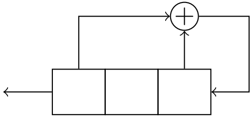


	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0

What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$

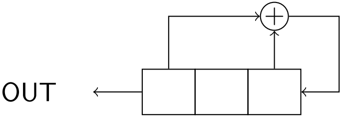
OUT



	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0

What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$



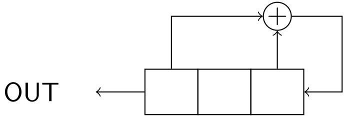
	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0
0	1	0	0	1

What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$

has period 7 with output $\overline{0\,0\,1\,1\,1\,0\,1}$.

This covers all non-zero starting states.



	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0
0	1	0	0	1
1	0	0	1	

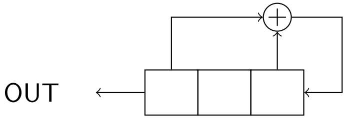
What is the period of $s_{j+3} = s_j + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$

has period 7 with output $\overline{0\,0\,1\,1\,1\,0\,1}$.

This covers all non-zero starting states.

For any LFSR, the all-zero state $S = (0\,0\,0\ \ldots\ 0)$ leads to output $\overline{0}$, of period 1 because $\sum c_i \cdot 0 = 0$.



	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0
0	1	0	0	1
1	0	0	1	

What is the period of $s_{j+3} = s_j + s_{j+2}$?

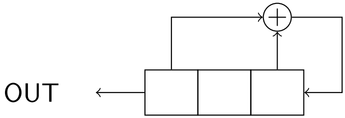
Starting state $S_0 = (0\ 0\ 1)$

has period 7 with output
$\overline{0\,0\,1\,1\,1\,0\,1}$.

This covers all non-zero starting states.

For any LFSR, the all-zero state
$S = (0\,0\,0\ \ldots\ 0)$
leads to output $\overline{0}$, of period 1
because $\sum c_i \cdot 0 = 0$.

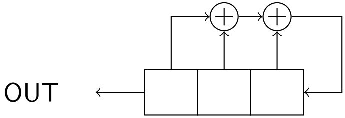
This means that period 7 is maximal
for a register of length 3, as $2^3 - 1 = 7$.



	0	0	1	1
0	0	1	1	1
0	1	1	1	0
1	1	1	0	1
1	1	0	1	0
1	0	1	0	0
0	1	0	0	1
1	0	0	1	

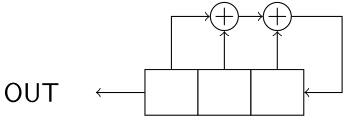
What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$



What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

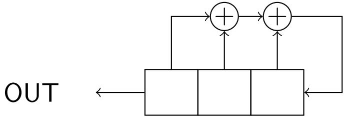
Starting state $S_0 = (0\ 0\ 1)$



0 0 1 1

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

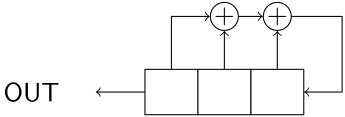
Starting state $S_0 = (0\ 0\ 1)$



	0	0	1	1
0	0	1	1	0

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

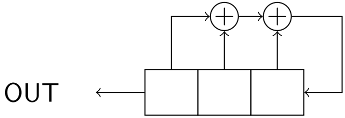
Starting state $S_0 = (0\ 0\ 1)$



	0	0	1	1
0	0	1	1	0
0	1	1	0	0

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$

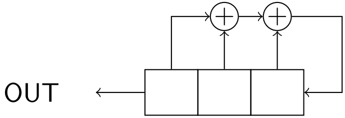


	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$ gives period 4 with output $\overline{0\,0\,1\,1}$.

This misses $2^3 - 4 = 4$ states.

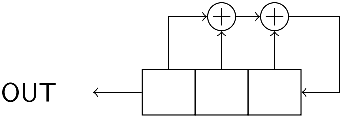


	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$ gives period 4 with output $\overline{0\,0\,1\,1}$.

This misses $2^3 - 4 = 4$ states.



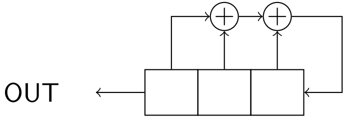
	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	
	1	1	1	1

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$ gives period 4 with output $\overline{0\,0\,1\,1}$.

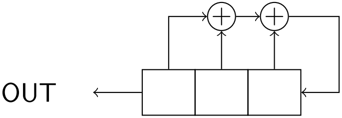
This misses $2^3 - 4 = 4$ states.

Starting state 1 1 1 gives period 1 with output $\overline{1}$



	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	
	1	1	1	1
1	1	1	1	

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?



Starting state $S_0 = (0\ 0\ 1)$ gives period 4 with output $\overline{0\,0\,1\,1}$.

This misses $2^3 - 4 = 4$ states.

Starting state $1\,1\,1$ gives period 1 with output $\overline{1}$

	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	

	1	1	1	1
1	1	1	1	

	1	0	1	0

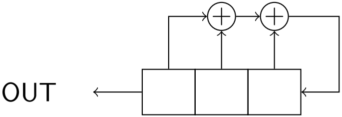
What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?

Starting state $S_0 = (0\ 0\ 1)$ gives period 4 with output $\overline{0\,0\,1\,1}$.

This misses $2^3 - 4 = 4$ states.

Starting state 1 1 1 gives period 1 with output $\overline{1}$

Starting state 1 0 1 gives period 2 with output $\overline{1\,0}$

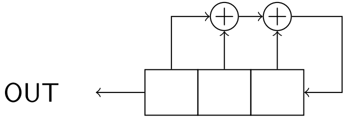


	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	

	1	1	1	1
1	1	1	1	

	1	0	1	0
1	0	1	0	1

What is the period of $s_{j+3} = s_j + s_{j+1} + s_{j+2}$?



Starting state $S_0 = (0\ 0\ 1)$
gives period 4 with output
$\overline{0\,0\,1\,1}$.

This misses $2^3 - 4 = 4$ states.

Starting state 1 1 1
gives period 1 with output $\bar{1}$

Starting state 1 0 1
gives period 2 with output $\overline{1\,0}$

Together with $\bar{0}$
we have now seen all 8 states.

Periods are 4,2,1,1
depending on starting state.

	0	0	1	1
0	0	1	1	0
0	1	1	0	0
1	1	0	0	1
1	0	0	1	

	1	1	1	1
1	1	1	1	

	1	0	1	0
1	0	1	0	1
0	1	0	1	

Security considerations

- An attacker knows the size of the register – there are n bits in the IV.
- The output bits have linear relations

$$s_{j+n} = \sum c_i s_{j+i},$$

Security considerations

- An attacker knows the size of the register – there are n bits in the IV.
- The output bits have linear relations

$$s_{j+n} = \sum c_i s_{j+i},$$

This means that obtaining $n-1$ outputs beyond the IV enables an attacker to compute the c_i using linear algebra.
($n-1$ because $c_0 = 1$ is known.)

Security considerations

- An attacker knows the size of the register – there are n bits in the IV.
- The output bits have linear relations

$$s_{j+n} = \sum c_i s_{j+i},$$

  This means that obtaining $n-1$ outputs beyond the IV enables an attacker to compute the c_i using linear algebra.

  ($n-1$ because $c_0 = 1$ is known.)
- This means that LFSRs alone do *not* satisfy the requirements we put on stream ciphers:

  A good stream cipher produces a stream of numbers that
  - *is unpredictable given any previous portion of the stream;*
  - *does not exhibit any non-random statistical properties.*

Security considerations

- An attacker knows the size of the register – there are n bits in the IV.
- The output bits have linear relations

$$s_{j+n} = \sum c_i s_{j+i},$$

  This means that obtaining $n-1$ outputs beyond the IV
  enables an attacker to compute the c_i using linear algebra.

  ($n-1$ because $c_0 = 1$ is known.)
- This means that LFSRs alone do *not* satisfy the requirements we put on stream ciphers:

  A good stream cipher produces a stream of numbers that
  - *is unpredictable given any previous portion of the stream;*
  - *does not exhibit any non-random statistical properties.*
- We can analyze LFSRs mathematically.
- LFSRs are used in combination with non-linear functions in stream cipher design.