LFSR

Demonstration of calculation of the states of a single linear feedback shift register

Clemens Brunner

clemens.brunner@student.uibk.ac.at

November 11, 2015

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Introduction

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Table of Content:

Outline

Linear feedback shift register

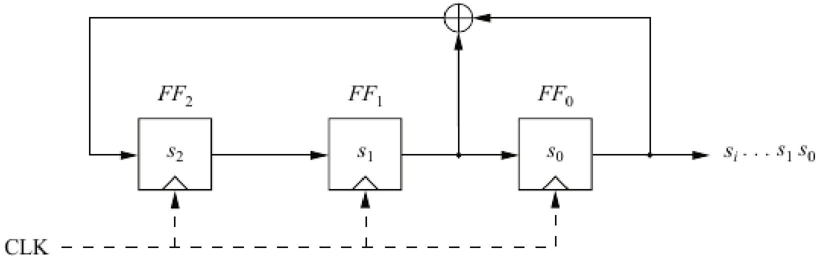

Figure : LFSR of degree 3 with initial values s_2, s_1, s_0 [Paar Christof 2009]

Linear feedback shift register

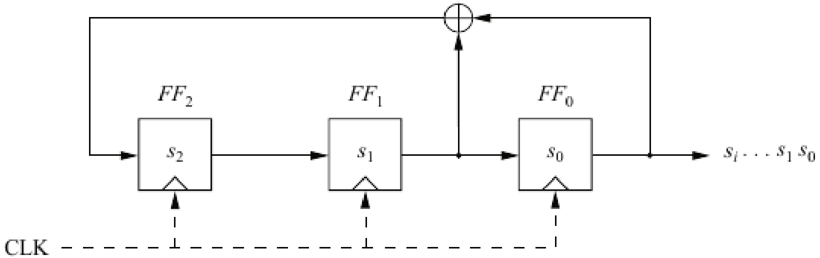

Figure : LFSR of degree 3 with initial values s_2, s_1, s_0 [Paar Christof 2009]

- Initial state: $(s_2, s_1, s_0) = (1, 0, 0)$

Linear feedback shift register

clk	FF_2	FF_1	$FF_0 = s_i$
0	1	0	0
1	0	1	0
2	1	0	1
3	1	1	0
4	1	1	1
5	0	1	1
6	0	0	1
7	1	0	0
8	0	1	0

Figure : Sequence of states of the LFSR [Paar Christof 2009]

Outline

Conceptual demonstration

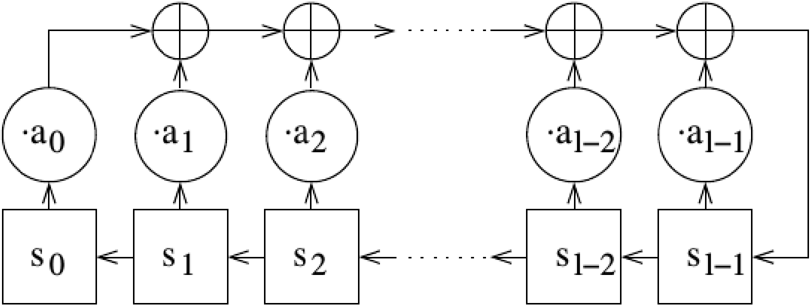

Figure : LFSR [Zenner Erik 2005]

Conceptual demonstration

- Feedback vector is unknown it is possible to calculate it using 2l consecutive output bits by solving l linear equations

$$\begin{pmatrix} s_0^i \\ s_1^i \\ \vdots \\ s_{l-2}^i \\ s_{l-1}^i \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{l-1} \end{pmatrix} \cdot \begin{pmatrix} s_0^{i-1} \\ s_1^{i-1} \\ \vdots \\ s_{l-2}^{i-1} \\ s_{l-1}^{i-1} \end{pmatrix}$$

Conceptual demonstration

- Feedback vector is unknown it is possible to calculate it using 2l consecutive output bits by solving l linear equations

$$\begin{pmatrix} s_0^i \\ s_1^i \\ \vdots \\ s_{l-2}^i \\ s_{l-1}^i \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{l-1} \end{pmatrix} \cdot \begin{pmatrix} s_0^{i-1} \\ s_1^{i-1} \\ \vdots \\ s_{l-2}^{i-1} \\ s_{l-1}^{i-1} \end{pmatrix}$$

Conceptual demonstration

- Feedback vector is unknown it is possible to calculate it using 2l consecutive output bits by solving l linear equations

$$
\begin{aligned}
s_l &= a_0 s_0 &+ a_1 s_1 + \ldots + a_{l-1} s_{l-1} \\
s_{l+1} &= a_0 s_1 &+ a_1 s_2 + \ldots + a_{l-1} s_l \\
\vdots &= \vdots &+ \vdots + \vdots + \vdots \\
s_{2l-1} &= a_0 s_{l-1} &+ a_1 s_l + \ldots + a_{l-1} s_{2l-2}
\end{aligned}
$$

Conceptual demonstration

- Feedback vector is unknown it is possible to calculate it using 2l consecutive output bits by solving l linear equations

$$
\begin{aligned}
s_l &= a_0 s_0 &&+ a_1 s_1 + \ldots + a_{l-1} s_{l-1} \\
s_{l+1} &= a_0 s_1 &&+ a_1 s_2 + \ldots + a_{l-1} s_l \\
\vdots &= \vdots &&+ \vdots + \vdots + \vdots \\
s_{2l-1} &= a_0 s_{l-1} &&+ a_1 s_l + \ldots + a_{l-1} s_{2l-2}
\end{aligned}
$$

- If the feedback vector is known it is possible to calculate all following state with knowing l arbitrary output bits.

Outline

Example: Calculation of states

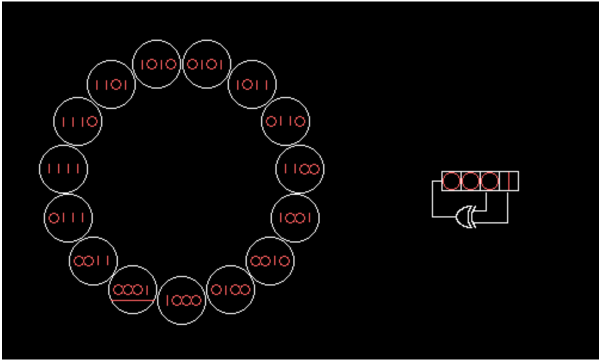

Figure : A 4-bit Fibonacci LFSR [Wikipedia]

Example: Calculation of states

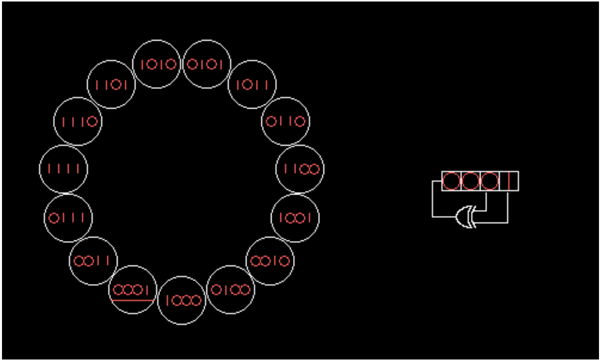

Figure : A 4-bit Fibonacci LFSR [Wikipedia]

- 2l output-bits: $s_0, s_1, \ldots, s_7$ are 10001001

Example: Calculation of states

- 2l output-bits: $s_0, s_1, \ldots, s_7$ are 10001001
- $$\begin{aligned} s_4 &= a_0 s_0 + a_1 s_1 + a_2 s_2 + a_3 s_3 \\ s_5 &= a_0 s_1 + a_1 s_2 + a_2 s_3 + a_3 s_4 \\ s_6 &= a_0 s_2 + a_1 s_3 + a_2 s_4 + a_3 s_5 \\ s_7 &= a_0 s_3 + a_1 s_4 + a_2 s_5 + a_3 s_6 \end{aligned}$$

Example: Calculation of states

- 2l output-bits: $s_0, s_1, \ldots, s_7$ are 10001001
- $$\begin{aligned} s_4 &= a_0 s_0 + a_1 s_1 + a_2 s_2 + a_3 s_3 \\ s_5 &= a_0 s_1 + a_1 s_2 + a_2 s_3 + a_3 s_4 \\ s_6 &= a_0 s_2 + a_1 s_3 + a_2 s_4 + a_3 s_5 \\ s_7 &= a_0 s_3 + a_1 s_4 + a_2 s_5 + a_3 s_6 \end{aligned}$$
- $$\begin{aligned} 1 &= a_0 1 + a_1 0 + a_2 0 + a_3 0 \\ 0 &= a_0 0 + a_1 0 + a_2 0 + a_3 1 \\ 0 &= a_0 0 + a_1 0 + a_2 1 + a_3 0 \\ 1 &= a_0 0 + a_1 1 + a_2 0 + a_3 0 \end{aligned}$$

Example: Calculation of states

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 1 & \mathbf{0} \\ 0 & 0 & 1 & 0 & \mathbf{0} \\ 0 & 1 & 0 & 0 & \mathbf{1} \end{array}\right] \xrightarrow{\text{Switch row 2 and 4}} \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 1 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 1 & 0 & \mathbf{0} \\ 0 & 0 & 0 & 1 & \mathbf{0} \end{array}\right]$$

- $a_0 = 1,\ a_1 = 1,\ a_2 = 0,\ a_3 = 0$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output:

Example: Calculation of states

- Feedback vector: $a_3 = 0$, $a_2 = 0$, $a_1 = 1$, $a_0 = 1$
- I initial sequence: $s_3 = 0$, $s_2 = 0$, $s_1 = 0$, $s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output:

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output:
- $s_4 = \mathbf{0} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{1} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1
- $s_4 = \mathbf{0} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{1} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1
- $s_5 = \mathbf{1} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 10
- $s_5 = \mathbf{1} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 10
- $s_6 = \mathbf{0} * 0 + \mathbf{1} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 100
- $s_6 = \mathbf{0} * 0 + \mathbf{1} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 100
- $s_7 = \mathbf{0} * 0 + \mathbf{0} * 0 + \mathbf{1} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1001
- $s_7 = \mathbf{0} * 0 + \mathbf{0} * 0 + \mathbf{1} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1001
- $s_8 = \mathbf{1} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{1} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 10011
- $s_8 = \mathbf{1} * 0 + \mathbf{0} * 0 + \mathbf{0} * 1 + \mathbf{1} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 10011
- $s_9 = \mathbf{1} * 0 + \mathbf{1} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 100110
- $s_9 = \mathbf{1} * 0 + \mathbf{1} * 0 + \mathbf{0} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 100110
- $s_{10} = \mathbf{0} * 0 + \mathbf{1} * 0 + \mathbf{1} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ \ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1001101
- $s_{10} = \mathbf{0} * 0 + \mathbf{1} * 0 + \mathbf{1} * 1 + \mathbf{0} * 1$

Example: Calculation of states

- Feedback vector: $a_3 = 0,\ a_2 = 0,\ a_1 = 1,\ a_0 = 1$
- I initial sequence: $s_3 = 0,\ s_2 = 0,\ s_1 = 0,\ s_2 = 1$
- Formula: $s_n = s_{n-1}a_3 + s_{n-2}a_2 + s_{n-3}a_1 + s_{n-4}a_0$
- Calculated output: 1001101...
- $s_{10} = \mathbf{0} * 0 + \mathbf{1} * 0 + \mathbf{1} * 1 + \mathbf{0} * 1$

Example: Calculation of states

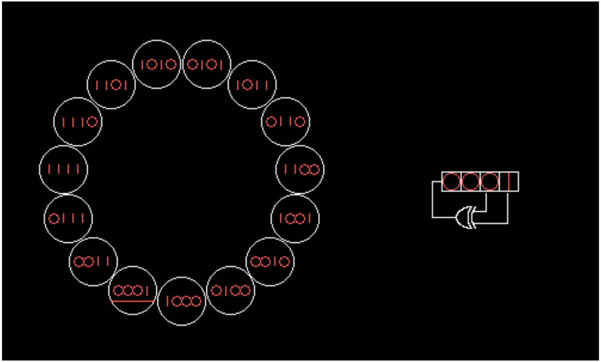

Figure : A 4-bit Fibonacci LFSR [Wikipedia]

Outline

Security of cipher based on LFSR

- Single LFSRs are insecure

Security of cipher based on LFSR

- ~~Single~~ LFSRs are secure

Security of cipher based on LFSR

- ~~Single~~ LFSRs are secure

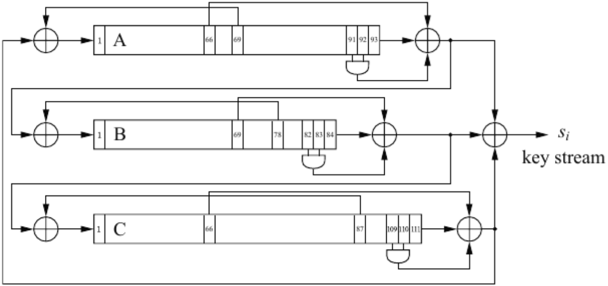

Figure : Trivium [Paar Christof 2009]

Conclusion

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Conclusion

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Conclusion

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra.
Derive conclusions for the security of ciphers based on LFSRs.

Conclusion

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra.
Derive conclusions for the security of ciphers based on LFSRs.

Conclusion

Demonstrate conceptually and by example how the state of a single linear feedback shift register (LFSR) can be calculated with algebra. Derive conclusions for the security of ciphers based on LFSRs.

Christof Paar and Jan Pelzl.
Understanding cryptography: a textbook for students and practitioners.
Springer Science & Business Media, 2009.

Erik Zenner.
On cryptographic properties of lfsr-based pseudorandom generators.
2005.

End

Any Questions?