Cryptographic Application of the Dynamic Linear Feedback Shift Registers (DLFSR)

A. Peinado*, A. Fúster-Sabater**
Contents

• Introduction
• Description of the DLFSR(m,n) Generator
• Characterization of the DLFSR(m,n) parameters:
  - Period
  - Linear complexity
  - Auto-correlation
  - Distribution of digits
• Analysis of DLFSR(5,16)
• Conclusions
Introduction

Pseudorandom Sequences for cryptographic application:

- Long period
- Difficult to predict
- Good distribution of 1’s and 0’s
- Two-fold auto-correlation

Generating devices:

The simplest: LFSR

Advantages:

- Long period $2^n - 1$
- Satisfies the Postulates of Golomb
- Easy to implement

Disadvantages:

- Extremely simple to predict
- Low Linear Complexity

2n bits are enough to generate $2^n - 1$
Introduction

Linear Complexity (LC)

- Amount of sequence needed to determine the whole sequence
- Length of the shortest LFSR that generates the sequence

Solutions:

- To apply non linear filters to the sequences
- To use non linear combinations of LFSR

Target:

- To keep the same properties
- To increase the LC

- Geffe generator
- Beth-Piper generator
- Multiple-speed generators
- Decimation generators
- eSTREAM generators (Trivium, Sosemanuk, Dragon, Decim, ...)
- DLFSR generator

DLFSR(m,n): Description

**Key Idea:**
Modification of the LFSR feedback polynomial in execution time

**Implementation:**
- **LFSR-n:** Generates the output sequence
- **DCPB:** Dynamic Characteristic Polynomial Block
- **LFSR-m:** Generates the control sequence
- **Decoder:** Selects the polynomial according to the present state of LFSR-m

**Primitive Polynomial**
Length of the sequence: \(2^m - 1\)

**Selection Table**
LFSR-m state | LFSR-n Polynomial
DLFSR(5,16): Description of an example

The configuration proposed in [1]

LFSR-5: Generates the control sequence

\[ x^5 + x^3 + 1 \] (Primitive)
Period \( 2^5 - 1 = 31 \)

Selection Table

<table>
<thead>
<tr>
<th>LFSR-m</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>11111</td>
<td>( p_1(x) = x^{16} + x^{15} + x^9 + x^6 + 1 )</td>
</tr>
<tr>
<td>01001</td>
<td>( p_2(x) = x^{16} + x^{13} + x^9 + x^6 + 1 )</td>
</tr>
<tr>
<td>00001</td>
<td>( p_3(x) = x^{16} + x^{10} + x^9 + x^6 + 1 )</td>
</tr>
<tr>
<td>00010</td>
<td>( p_4(x) = x^{16} + x^{12} + x^9 + x^6 + 1 )</td>
</tr>
</tbody>
</table>

LFSR-16: Generates the output sequence

DCPB: Dynamic Characteristic Polynomial Block

All the polynomials are primitive and differ just in one coefficient

DLFSR Generator
DLFSR(5,16) : Description of an example

**Selection Table**

<table>
<thead>
<tr>
<th>LFSR-m</th>
<th>LFSR-n</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>11111</td>
<td>p₁(x)</td>
<td>(x^{16} + x^{15} + x^{9} + x^{6} + 1)</td>
</tr>
<tr>
<td>01001</td>
<td>p₂(x)</td>
<td>(x^{16} + x^{13} + x^{9} + x^{6} + 1)</td>
</tr>
<tr>
<td>00001</td>
<td>p₃(x)</td>
<td>(x^{16} + x^{10} + x^{9} + x^{6} + 1)</td>
</tr>
<tr>
<td>00010</td>
<td>p₄(x)</td>
<td>(x^{16} + x^{12} + x^{9} + x^{6} + 1)</td>
</tr>
</tbody>
</table>

p₁(x) : 9 consecutive times
p₂(x) : 5       “                “
p₃(x) : 1        “                “
p₄(x) : 16      “                “

DLFSR Generator
DLFSR(m,n) : Linear Complexity (I)

- \(v(t)\) LFSR-n state vector at time \(t\), \(v(t) = (v_0(t), ..., v_{n-1}(t))\)
- \(s(t)\) Sequence generated by the DLFSR, \(s(t) = v_0(t)\)
- \(l = 2^m - 1\) period of the LFSR-m sequence

Decimated sequence

\[ w_0(0) = s(0) \]
\[ w_0(1) = s(l) \]
\[ w_0(2) = s(2l) \]

\[ v((t+1)/l) = v(t/l)M \]
\[ M = \prod_{i=0}^{l-1} A_i \]

\(A_i\) matrix whose characteristic polynomial is the LFSR-n feedback polynomial at time \(i\)

\[ v((t+1)/l) = v(0)M^{t+1} \]

\[ w_0(t) = \pi v(0)M^t \]
Characteristic polynomial of $M$: $c(x) = \sum_{i=0}^{n} c_i x^i$

$$\sum_{i=0}^{n} c_i w_0(t + i) = \pi v(0) M^t c(M) = 0$$

$s(t)$ can be obtained by interleaving $l$ different sequences $w_j(t) = s(tl + j)$ each of them with LC $\leq n$

$$LC(s) \leq n \cdot l = n \left(2^m - 1\right)$$
DLFSR(m,n) : Period

**Computing the period of s(t):**

\[
T(s) = \text{lcm} \left( T(w_j) \right) \left( 2^m - 1 \right)
\]

\[0 \leq j < 2^m - 1\]

The period \(T(w_j)\) of each decimated sequence \(w_j(t)\) is determined by the matrix \(M_j\) via its characteristic polynomial \(c_j(x)\)

\[
T(s) = \text{lcm} \left( \text{per} \left( c_j(x) \right) \right) \left( 2^m - 1 \right)
\]

All the matrices \(M_j\) are cyclic shifts of the matrix \(M_0\)

\[
M_0 = A_0 A_1 A_2 A_3 \cdots A_{l-1}
\]

\[
M_1 = A_1 A_2 A_3 \cdots A_{l-1} A_0
\]

\[
M_2 = A_3 \cdots A_{l-1} A_0 A_1 A_2
\]

All of them have the same characteristic polynomial \(c(x)\)

\[
T(s) = \text{per} \left( c(x) \right) \left( 2^m - 1 \right)
\]

The period will be maximum when \(c(x)\) is a primitive polynomial

\[
T(s) \leq \left( 2^n - 1 \right) \left( 2^m - 1 \right)
\]
Analysis of DLFSR(5,16)

**Linear Complexity:**

Upper bound: $LC \leq n \cdot (2^m-1) = 16 \cdot 31 = 496$
Massey-Berlekamp algorithm: $\leq 496$

**Maximum period:**

$$T(s) = \text{per}(c(x))(2^m - 1) = \text{per}(c(x)) \cdot 31$$

$$M = \prod_{i=0}^{l-1} A_i = M_0 = A_1^9 A_2^5 A_3 A_4^{16}$$

$$c(x) = x^{16} + x^{15} + x^{11} + x^{10} + x^9 + x^4 + x + 1$$

$$= (x+1)^2(x^4 + x + 1)(x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + 1)$$

$$\text{per}(c(x)) = \text{lcm}(2, 15, 1023) = 2 \cdot 5115 = 10230$$

**Primitive**

$$T(s) = 10230 \cdot 31 = 317130$$
Analysis of DLFSR(5,16)

There are other configurations generating sequences with greater periods

\[ M = \prod_{i=0}^{l-1} A_i = M_0 = A_2^5 A_3 A_4^{16} \]

\[ c(x) = x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^7 + x^6 + x + 1 \]
\[ = (x^6 + x^5 + 1)(x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1) \]

Primitive

\[ \text{per}(c(x)) = \text{lcm}(2^6 - 1, 2^{10} - 1) = 21483 \]

\[ T(s) = 31 \cdot 21483 = 665973 \]

1's and 0's Distribution

Practically ideal

Auto-correlation

Periodic peaks with amplitude 0.2

Cross-correlation

Peaks with very remarkable periodicity
1’s and 0’s distribution

Run distribution of the interleaved sequence
Auto-correlation

Autocorrelation
Sequence Length: 158564

Distance = 31713 = 1023 \cdot 31

Auto-correlation of the interleaved sequence
Cross-correlation of the interleaved sequence

Distance = 31713 = 1023 \cdot 31
Conclusions

• Characterization of the DLFSR(m,n) generator
  - Upper bounds on the linear complexity and maximum period
  - Estimations on the auto-correlation

• Study of the proposed configuration DLFSR(5,16)
  - Confirms the DLFSR(m,n) as a generator of interleaved sequence
  - Proves that the original configuration is not optimal

• Considerations on the design of DLFSR(m,n)
  - The upper bound on the LC is independent of the table of polynomials. It only depends on the length of the control sequence and the LFSR-n
  - It is not easy to find a configuration satisfying particular requirements on period and LC of the generated sequence

• Possible cryptographic application
  - Although the upper bound is met, LC of the generated sequence will always be low for cryptography