

Solutions to Assignment 3

Question 1

An upper bound is given by the product of periods of three LFSRs, i.e., $7 \times 15 \times 31$, and a low bound happens when both the initial states of the LFSRs with degrees 4 and 5 are loaded as zeros, which is 7.

Question 2

(a) The WG cipher has the following randomness properties:

- long period $(2^{319} - 1)$ balanced property;
- 2-level autocorrelation property;
- ideal t -tuple distribution $(1 \leq t \leq 11)$ property;
- large linear span; and
- cross-correlation with m -sequence is 3-valued etc.

(b) Use Method 2.

Let $n \not\equiv 0 \pmod 3$, α be a primitive element of \mathbb{F}_{2^n} , and $t(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$, $x \in \mathbb{F}_{2^n}$, where the q_i 's are given by

| | |
|--------------|---|
| $n = 3k - 1$ | $q_1 = 2^k + 1$ $q_2 = 2^{2k-1} + 2^{k-1} + 1$ $q_3 = 2^{2k-1} - 2^{k-1} + 1$ $q_4 = 2^{2k-1} + 2^k - 1$ |
| $n = 3k - 2$ | $q_1 = 2^{k-1} + 1$ $q_2 = 2^{2k-2} + 2^{k-1} + 1$ $q_3 = 2^{2k-2} - 2^{k-1} + 1$ $q_4 = 2^{2k-1} - 2^{k-1} + 1$ |

The function defined by

$$f(x) = \text{Tr}(t(x+1) + 1), x \in \mathbb{F}_{2^n}$$

is called the WG transformation of $\text{Tr}(t(x))$.

If $n = 7 = 3 * 3 - 2$, then $k = 3$, $q_1 = 5$, $q_2 = 21$, $q_3 = 13$, $q_4 = 29$. Hence the WG transform is $f(x) = \text{Tr}(t(x+1) + 1)$, $x \in \mathbb{F}_{2^n}$, where $t(x) = x + x^5 + x^{21} + x^{13} + x^{29}$, $x \in \mathbb{F}_{2^n}$

If $n = 8 = 3 * 3 - 1$, then $k = 3$, $q_1 = 9$, $q_2 = 37$, $q_3 = 29$, $q_4 = 39$. Hence the WG transform is $f(x) = \text{Tr}(t(x+1) + 1)$, $x \in \mathbb{F}_{2^n}$, where $t(x) = x + x^9 + x^{37} + x^{29} + x^{39}$, $x \in \mathbb{F}_{2^n}$

⁰Copyright ©2009 Guang Gong. All rights reserved. May be freely reproduced for educational or personal use.

Question 3

For fixed initial state of LFSR $(a_0, a_1, a_2, a_3) = (0, 0, 0, 1)$ and different initial states of NLFSR ranging from 0000 – 1111, output sequences and periods are shown in Table 1:

Table 1: The output sequences and periods of these sequences for $(a_0, a_1, a_2, a_3) = (0, 0, 0, 1)$

| initial state of NLFSR (b_0, b_1, b_2, b_3) | Output sequences | Periods |
|---|---|---------|
| 0001 | 1001000011111000100000111111100101010010000100100101101111100 | 60 |
| 0010 | 1000001111111001010100100001001001011011111001001000011111000 | 60 |
| 0011 | 1010101100000110110011100001010110111110000000 | 45 |
| 0100 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 0101 | 1010101100000110110011100001010110111110000000 | 45 |
| 0110 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 0111 | 1010101100000110110011100001010110111110000000 | 45 |
| 1000 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1001 | 1010101100000110110011100001010110111110000000 | 45 |
| 1010 | 1010101100000110110011100001010110111110000000 | 45 |
| 1011 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1100 | 1010101100000110110011100001010110111110000000 | 45 |
| 1101 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1110 | 1010101100000110110011100001010110111110000000 | 45 |
| 1111 | 101010010000100100101101111100100100001111000100000111111100 | 60 |

For fixed initial state of LFSR $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$ and different initial states of NLFSR ranging from 0000 – 1111, output sequences and periods are shown in Table 2:

Table 2: The output sequences and periods of these sequences for $(a_0, a_1, a_2, a_3) = (1, 0, 1, 0)$

| initial state of NLFSR (b_0, b_1, b_2, b_3) | Output sequences | Periods |
|---|--|---------|
| 0001 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 0010 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 0011 | 101010110000011011001110000101011011110000000 | 45 |
| 0100 | 100100001111000100000111111100101010010000100100101101111100 | 60 |
| 0101 | 101010110000011011001110000101011011110000000 | 45 |
| 0110 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 0111 | 101010110000011011001110000101011011110000000 | 45 |
| 1000 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1001 | 101010110000011011001110000101011011110000000 | 45 |
| 1010 | 101010110000011011001110000101011011110000000 | 45 |
| 1011 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1100 | 101010110000011011001110000101011011110000000 | 45 |
| 1101 | 100101101111100100100001111000100000111111100101010010000100 | 60 |
| 1110 | 101010110000011011001110000101011011110000000 | 45 |
| 1111 | 100000111111100101010010000100100101101111100100100001111000 | 60 |