

Assignment 3 (Topic 4. Stream Ciphers)

1. 12-bit A5: In the A5 structure, let three LFSRs have degrees 3, 4 and 5, respectively. The tap positions are 1, 2 and 3 in each of those LFSRs, respectively.
 - (a) What is the upper bound of the periods of the output sequences of 12-bit A5?
 - (b) Determine a lower bound of the periods.

2. WG cipher:

Mathematical parameters

m	Bit-width of cipher
$g(x)$	Generating polynomial for $GF(2^m)$
$p(x)$	Primitive polynomial for LFSR
l	Degree of $p(x)$.

$WG(x) = t(x + 1) + 1$ $t(x) = x + x^{q_1} + x^{q_2} + x^{q_3} + x^{q_4}$ <p style="margin: 0;">where $x \in GF(2^m)$</p>

The cipher is referred to as an m -bit WG cipher.

Method I for the definition of q_i 's: Find k such that $3k \equiv 1 \pmod{m}$.

$$\begin{aligned}
 q_1 &= 2^k + 1 \\
 q_2 &= 2^{2k} + 2^k + 1 \\
 q_3 &= 2^{2k} - 2^k + 1 \\
 q_4 &= 2^{2k} + 2^k - 1.
 \end{aligned}$$

This set produces both $t(x)$ and $WG(x)$ are permutations over $GF(2^m)$.

Method II for the definition of q_i 's:

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

The function defined by

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

is called the *Welch-Gong transformation* of $Tr(t(x))$, or the *WG transformation* for short where q_i can be determined by either the above two methods. Note that $f(x)$ is a function from \mathbb{F}_{2^n} to \mathbb{F}_2 .

- (a) List randomness properties of WG cipher as many as you can.
 - (b) What is the WG transformation for $n = 7$ and $n = 8$?
3. 4-bit Grain 2: In the structure of Grain 2, let both the LFSR and NLFSR have degree 4. The characteristic polynomial of the LFSR is given by $x^4 + x + 1$ and output is $\{a_i\}$. The feedback of the NLFSR is given by $g(x_0, x_1, x_2, x_3) = x_0 + x_1x_2 + x_2x_3$ and the output is $\{b_i\}$ where the feedback bit is $b_{i+4} = a_i + g(b_i, b_{i+1}, b_{i+2}, b_{i+3})$. The output of the generator is given by

$$s_i = b_i + b_{i+3} + a_i a_{i+2}, i = 0, 1, \dots$$

Answer one of the following two questions.

- (a) List all output sequences of the generator for fixed initial states 0001 and 1010 in the LFSR.
- (b) Determine the periods of those sequences or some lower and upper bounds of those sequences.