Introduction to Cryptography: Assignment 2

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a) Considering an exhaustive key search, the security strength is 4 bits for the top LSFR and 8 bits for the bottom LSFR, so in total the security strength is 12 bits.

(b)

$$
\begin{aligned}
s_0 &= 0101 & & \\
s_1 &= 1011 & z_0 &= 1 \\
s_2 &= 1100 & z_1 &= 1 \\
s_3 &= 0110 & z_2 &= 0 \\
s_4 &= 0011 & z_3 &= 0 \\
s_5 &= 1000 & z_4 &= 1 \\
s_6 &= 0100 & z_5 &= 0 \\
s_7 &= 0010 & z_6 &= 0 \\
s_8 &= 0001 & z_7 &= 0 \\
s_9 &= 1001 & z_8 &= 1 \\
s_{10} &= 1101 & z_9 &= 1 \\
s_{11} &= 1111 & z_{10} &= 1 \\
s_{12} &= 1110 & z_{11} &= 1 \\
s_{13} &= 0111 & z_{12} &= 0 \\
s_{14} &= 1010 & z_{13} &= 1 \\
s_{15} &= 0101 & z_{14} &= 0 \\
s_{16} &= 1011 & z_{15} &= 1
\end{aligned}
$$

$$z = 1100100011110101$$

(c)

$$
\begin{aligned}
(11001000 + z_0) \quad \bmod 2^8 &= 10010001 \\
(11110101 + z_1) \quad \bmod 2^8 &= 01000100
\end{aligned}
$$

Solving z_0 and z_1 gives:

$$
\begin{aligned}
z_0 &= 256 + 145(10010001) - 200(11001000) \quad &&=201 \\
z_1 &= 256 + 68(01000100) - 245(11110101) \quad &&=79
\end{aligned}
$$

201 in binary = 11001001
79 in binary = 01001111
Thus the first sixteen bits of the output stream for the 8-bit LSFR = 1100100101001111

(d) The table displays the steps taken to regain the current state s^8 and $s^0 = (s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7)$.

s^0	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	$s_7 = z_0 = 1$
s^1	1	$s_0 + 1$	s_1	$s_2 + 1$	s_3	$s_4 + 1$	s_5	s_6	$s_6 = z_1 = 1$
s^2	1	0	$s_0 + 1$	$s_1 + 1$	$s_2 + 1$	$s_3 + 1$	$s_4 + 1$	s_5	$s_5 = z_2 = 0$
s^3	0	1	0	$s_0 + 1$	$s_1 + 1$	$s_2 + 1$	$s_3 + 1$	$s_4 + 1$	$s_4 + 1 = z_3 = 0$
s^4	0	0	1	0	$s_0 + 1$	$s_1 + 1$	$s_2 + 1$	$s_3 + 1$	$s_3 + 1 = z_4 = 1$
s^5	1	1	0	0	0	s_0	$s_1 + 1$	$s_2 + 1$	$s_2 + 1 = z_5 = 0$
s^6	0	1	1	0	0	0	s_0	$s_1 + 1$	$s_1 + 1 = z_6 = 0$
s^7	0	0	1	1	0	0	0	s_0	$s_0 = z_7 = 1$
s^8	1	1	0	0	1	1	0	0	

$s^0 = (1, 1, 1, 0, 1, 0, 1, 1)$
$s^8 = (1, 1, 0, 0, 1, 1, 0, 0)$

(e) The key, of the 8-bit LFSR, that was derived from the 4-bit LFSR has to provide two 8-bit outputs that, when added up to their 4-bit counterpart, add up to the values of Z. This was not the case with the key of 0101, thus the guess was incorrect.

(f) The keys are 1111 and 11111111 respectively, see the code provided.

```
Testing key for 4-bit LSFR: 1111
    Output 4-bit LSFR: 10101100 10001111
    Output 8-bit LSFR: 11100101 10110101
    Key for 8-bit LSFR based on first byte: 11111111
    The rest of the output matches: 1110010110110101 == 1110010110110101
```