T-79.5501 Cryptology Spring 2009

Homework 5

Tutor : Joo Y. Cho
joo.cho@tkk.fi

5th March 2009

Q1. Using the Berlekamp-Massey Algorithm find an LFSR that generates the sequence:

`0 0 0 1 1 1 0 0 .`

Compare your solution with the polynomial found in HW4.

$$L_{k+1} = \max\{L_k,\ k+1-L_k\}$$
$$f^{k+1}(x) = x^{L_{k+1}-L_k}\, f^k(x) + x^{L_{k+1}-k+m-L_m}\, f^m(x)$$

Running the Berlekamp-Massey algorithm we get:

k	z_{k-1}	L_k	$f^{(k)}$	observing z_k
2	0	0	1	
3	0	0	1	$z_3 = 1$ (the first nonzero term), set $L_4 = 4$ and $f^{(4)}(x) = x^4 + 1$
4	1	4	$x^4 + 1$	does not work for $z_4 = 1$, change: $L_5 = \max\{4, 5-4\} = 4$ and $f^{(5)} = x^0(x^4 + 1) + x^{4-4+3} \cdot 1$
5	1	4	$x^4 + x^3 + 1$	OK for $z_5 = 1$, no changes
6	1	4	$x^4 + x^3 + 1$	does not work for $z_6 = 0$, change: $L_7 = \max\{4, 7-4\} = 4$ and $f^{(7)} = x^0(x^4 + x^3 + 1) + x^{4-6+3} \cdot 1$
7	0	4	$x^4 + x^3 + x + 1$	OK for $z_7 = 0$, no changes
8	0	4	$x^4 + x^3 + x + 1$	no more sequence

Q2. Consider the 4-bit to 4-bit permutation π_S defined as follows:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E

(This is the fourth row of the DES S-box S_4.) Denote by (x_1, x_2, x_3, x_4) and by (y_1, y_2, y_3, y_4) the input bits and output bits respectively. Find the output bit y_j for which the bias of $x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus y_j$ is the largest.

x_1	x_2	x_3	x_4	S_1	y_1	y_2	y_3	y_4	$x_1 \oplus x_2 \oplus x_3 \oplus x_4$
0	0	0	0	3	0	0	1	1	0
0	0	0	1	15	1	1	1	1	1
0	0	1	0	0	0	0	0	0	1
0	0	1	1	6	0	1	1	0	0
0	1	0	0	10	1	0	1	0	1
0	1	0	1	1	0	0	0	1	0
0	1	1	0	13	1	1	0	1	0
0	1	1	1	8	1	0	0	0	1
1	0	0	0	9	1	0	0	1	1
1	0	0	1	4	0	1	0	0	0
1	0	1	0	5	0	1	0	1	0
1	0	1	1	11	1	0	1	1	1
1	1	0	0	12	1	1	0	0	0
1	1	0	1	7	0	1	1	1	1
1	1	1	0	2	0	0	1	0	1
1	1	1	1	14	1	1	1	0	0
number n_i					10	4	10	8	
bias value					$\frac{1}{8}$	$-\frac{1}{4}$	$\frac{1}{8}$	0	

Q3. Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables which take on values from the set $\{0, 1\}$. We use ϵ_i to denote the bias of $\mathbf{X}_i$, $\epsilon_i = \Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, for $i = 1, 2$. Prove that the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent if and only if $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

A3. Claim: The random variables X_1 and $X_1 \oplus X_2$ are independent if and only if $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.
Suppose that X_1 and X_2 are independent random variables. Let ϵ_{12} denote the bias of $X_1 \oplus X_2$ and ϵ_{112} the bias of $X_1 \oplus (X_1 \oplus X_2)$.
[“$\Rightarrow$”]
We prove that $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$ if the random variables X_1 and $X_1 \oplus X_2$ are independent. By the Piling-Up Lemma, we have $\epsilon_{12} = 2\epsilon_1\epsilon_2$ and $\epsilon_{112} = 2\epsilon_1\epsilon_{12}$. Hence,

$$\epsilon_{112} = 2\epsilon_1 2\epsilon_1\epsilon_2 = 4\epsilon_1^2\epsilon_2.$$

Since $X_1 \oplus (X_1 \oplus X_2) = X_2$, we have $\epsilon_{112} = \epsilon_2$, and thus

$$4\epsilon_1^2\epsilon_2 = \epsilon_2.$$

This equation holds if and only if either $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$.

[$\Leftarrow$]
We prove that X_1 and $X_1 \oplus X_2$ are independent if $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$. The proof makes use of the converse of the Piling-Up Lemma. Since X_1 and X_2 are independent random variables, we have

$$2\epsilon_1\epsilon_{12} = 4\epsilon_1^2\epsilon_2 = \begin{cases} 0 & \text{if } \epsilon_2 = 0, \\ \epsilon_2 & \text{if } \epsilon_1 = \pm\frac{1}{2}. \end{cases}$$

In other words, $2\epsilon_1\epsilon_{12} = \epsilon_2$ if $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$. Because $\epsilon_{112} = \epsilon_2$, we get $\epsilon_{112} = 2\epsilon_1\epsilon_{12}$. By the converse of the Piling-Up Lemma, X_1 and $X_1 \oplus X_2$ are independent.

Q4. Suppose that $w \in \{0,1\}^n$. Show that

$$\sum_{x \in \{0,1\}^n} (-1)^{w \cdot x} = \begin{cases} 0, \text{ for } w \neq 0 \\ 2^n, \text{ for } w = 0 \end{cases}$$

Hint. Determine the number of $x \in \{0,1\}^n$ such that $w \cdot x = 0$.

If $w = 0$, we get

$$\sum_{x \in \{0,1\}^n} (-1)^{w \cdot x} = \sum_{x \in \{0,1\}^n} 1 = 2^n.$$

If $w \neq 0$, we get

$$\sum_{x \in \{0,1\}^n} (-1)^{w \cdot x} = \sum_{x \,:\, w \cdot x = 0} 1 + \sum_{x \,:\, w \cdot x = 1} (-1) = 2^{n-1} - 2^{n-1} = 0.$$

This is true because there is an equal amount of $x \in \{0, 1\}^n$ that satisfy $w \cdot x = 0$ and $w \cdot x = 1$ for $w \neq 0$.

To prove the latter case more strictly, we use induction on the number of coordinates in $w = (w_1, \ldots, w_n)$ and $x = (x_1, \ldots, x_n)$. If $n = 1$, we have $w = 1 \neq 0$, and it follows that

$$\sum_{x \in \{0,1\}} (-1)^{w \cdot x} = (-1)^0 + (-1)^1 = 0.$$

Hence, the claim is true for $n = 1$. Suppose that the claim is true for $n = k \geq 1$. We show that the claim is true for $n = k + 1$. Denote $w' = (w_1, \ldots, w_k)$ and $x' = (x_1, \ldots, x_k)$. Dividing the sum into separate parts based on whether $x_{k+1} = 0$ or $x_{k+1} = 1$, we get

$$\begin{aligned}
\sum_{x \in \{0,1\}^{k+1}} (-1)^{w \cdot x} &= \sum_{x' \in \{0,1\}^k} (-1)^{w' \cdot x' \oplus w_{k+1} \cdot 0} + \sum_{x' \in \{0,1\}^k} (-1)^{w' \cdot x' \oplus w_{k+1} \cdot 1} \\
&= \underbrace{\sum_{x' \in \{0,1\}^k} (-1)^{w' \cdot x'}}_{=0} + (-1)^{w_{k+1}} \underbrace{\sum_{x' \in \{0,1\}^k} (-1)^{w' \cdot x'}}_{=0} \\
&= 0.
\end{aligned}$$

This proves the claim for $n = k + 1$.

Q5. Consider the example linear attack in the textbook, Section 3.3.3. For S_2^2 replace the random variable $\mathbf{T}_2$ by $\mathbf{U}_6^2 \oplus \mathbf{V}_8^2$. Then in the third round the random variable $\mathbf{T_3}$ is not needed. What is the final random variable corresponding to Equation (3.3) and what is its bias?

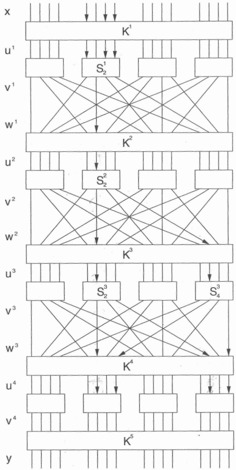

FIGURE 3.3
A linear approximation of a substitution-permutation network

A5.

- $\mathbf{T'}_2 = \mathbf{U}_6^2 \oplus \mathbf{V}_8^2$
- $\mathbf{T_3}$ is not needed. Hence, the arrows through S_2^3 are removed.
- $\mathbf{U}_6^2$ and $\mathbf{U}_{14}^4$ are removed.
- The new final variable is

$$\mathbf{X}_5 \oplus \mathbf{X}_7 \oplus \mathbf{X}_8 \oplus \mathbf{U}_8^4 \oplus \mathbf{U}_{16}^4.$$

- The bias of the new variable $\mathbf{T'}_2$: in the table of the S-box (Figure 3.2) $a = 0100 = 4$ and $b = 0001 = 1$. Hence, $N_L(a,b) = N_L(4,1) = 10$. The bias $\epsilon'_2 = 10/16 - 1/2 = 1/8$.
- The biases of approximation is $2^{3-1}\epsilon_1\epsilon'_2\epsilon_4 = 4(1/4)(1/8)(-1/4) = -1/32$.

Q6.

Consider the finite field $GF(2^3) = \mathbf{Z}_2[x]/(f(x))$ with polynomial $f(x) = x^3 + x + 1$ (see Stinson 6.4).

1. Compute the look-up table for the inversion function $g : z \mapsto z^{-1}$ in $GF(2^3)$, where we set $g(0) = 0$.
2. Compute the algebraic normal form of the Boolean function defined by the least significant bit of the inversion function.

A6-a. The multiplication table of the finite field $GF(2^3) = \mathbf{Z}_2[x]/(x^3 + x + 1)$ is given on page 253 of the textbook. Using it we can, given a nonzero element, find another element such that the product is equal to 1 = 001. We get:

z	z^{-1}
000	000
001	001
010	101
011	110
100	111
101	010
110	011
111	100

A6-a. Another approach to create this function table is to express the seven elements of the multiplicative group of $\mathbf{Z}_2[x]/(x^3+x+1)$ as powers of the element $x = 010$:

k	x^k
0	$x^0 = 001$
1	$x = 010$
2	$x^2 = 100$
3	$x^3 = 011$
4	$x^4 = 110$
5	$x^5 = 111$
6	$x^6 = 101$

The $g(z) = g(x^k) = x^{-k} = x^{7-k}$, for all $k = 0, 1, \ldots 6$ as the order of the multiplicative group of $\mathbf{Z}_2[x]/(x^3+x+1)$ is seven.

A6-b. Using the ANF algorithm (Lecture 6) we get

k	b_3	b_2	b_1	$f(b_1, b_2, b_3)$	
	x_3	x_2	x_1		$g(x_1, x_2, x_3)$
0	0	0	0	0	0
1	0	0	1	1	x_1
2	0	1	0	1	$x_1 \oplus x_2$
3	0	1	1	0	$x_1 \oplus x_2$
4	1	0	0	1	$x_1 \oplus x_2 \oplus x_3$
5	1	0	1	0	$x_1 \oplus x_2 \oplus x_3$
6	1	1	0	1	$x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3$
7	1	1	1	0	$x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3$