Cryptography **3 Sep 2015**

Lecture 8: LFSR II; Boolean Functions

Lecturer: Goutam Paul *Scribe: Shion Samadder Chaudhury*

In this lecture we continue our study of the LFSR, how to introduce non-linearity in the system and we look at some examples of cryptographic properties of Boolean functions.

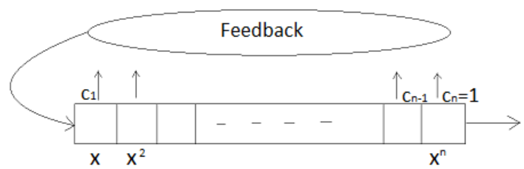

Figure 8.1: An n- bit LFSR

8.1 Characteristic polynomial and Minimal polynomial

Definition 8.1 *For the n-bit LFSR as in the figure above the polynomial :* $c(x) = x^n + c_{n-1}x^{n-1} + ... + c_1x + 1$ *is called the* *connection polynomial* *of the LFSR.*

Definition 8.2 *Let* $\vec{s} = (s_0, s_1, s_2, ...)$ *be an LFSR sequence. Then the* *shift operator* L *is defined as :* $L(\vec{s}) := (s_1, s_2, ...)$.

Using composition of the shift operators we can talk about powers $L, L^2, L^3...$ and can consider polynomials of shift operators.

Definition 8.3 *A polynomial* f *such that* $f(L)\vec{s} = \vec{0}$ *is called a* *characteristic polynomial* *of the sequence* $\vec{s}$.

Definition 8.4 *The characteristic polynomial* $\vec{s}$ *of minimum degree is called the* *minimal polynomial* *of* $\vec{s}$.

Now we have the following propositions.

Proposition 8.5 *If* $\vec{s}$ *is a sequence over a finite field* F*, the connection polynomial* $c(x)$ *of the LFSR is a minimal polynomial of* $\vec{s}$ *if* $c(x)$ *is irreducible.*

We note that

- If $\vec{s}$ has period r, then $x^r - 1$ is a characteristic polynomial of $\vec{s}$.

Definition 8.6 *The* *period of a polynomial* $g(x) \in F_p[x]$ *is defined as the minimum integer* e *such that* $g(x) | x^e - 1$.

Proposition 8.7 *If $m(x)$ is the minimal polynomial of a sequence $\vec{s}$, then $period(m(x)) = period(\vec{s})$.*

- From 8.5 and 8.7, if we want to maximize the period, then $period(\vec{s}) = p^n - 1$.
- Hence from 8.7 we have $period(m(x)) = period(\vec{s})$.
- So, from 8.5, $period(c(x)) = p^n - 1$ if the sequence is produced from an LFSR of connection polynomial $c(x)$.
- Definition 8.6 implies that the minimum integer e such that $c(x)|x^e - 1$ is $e = p^n - 1$. Such a polynomial is called a primitive polynomial.

From the above discussion, to choose a connection we need to choose a primitive polynomial.

8.2 Problem of LFSR

LFSR is safe for ciphertext only attacks. Suppose we have an LFSR sequence : $s_0, s_1, s_2, ...$ We XOR with the message bits to get the ciphertext. Suppose we get a portion of the text. Then we have the following system of equations.

$$s_n = a_0 s_0 + a_1 s_1 + ... + a_{n-1} s_{n-1}$$

$$s_{n+1} = a_0 s_1 + a_1 s_2 + ... + a_{n-1} s_n$$

$$................$$

$$s_{2n-1} = a_0 s_{n-1} + a_1 s_n + ... + a_{n-1} s_{2n-2}$$

Treating the a_i's as unknowns, we get a system of n equations in n unknowns given by :

$$\begin{pmatrix} s_n \\ s_{n+1} \\ . \\ . \\ . \\ s_{2n-1} \end{pmatrix} = \begin{pmatrix} s_0 & s_1 & . & . & . & s_{n-1} \\ s_1 & s_2 & . & . & . & s_n \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ s_{n-1} & s_{n-2} & . & . & . & s_{2n-2} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ . \\ . \\ . \\ a_{n-1} \end{pmatrix}$$

Since the $n \times n$ matrix on the R.H.S is symmetric, it is invertible. So the a_i's, i.e the connections are completely determined which is the attacker's advantage.

Definition 8.8 *The Linear Complexity of a sequence is the minimum length LFSR that produces the sequence.*

If a sequence has length n, then its linear complexity $\leq \frac{n}{2}$.

From the above discussion, purely linear feedback is not good. Hence we introduce non-linearity in the system. We shall formally define non-linearity of a Boolean function in the next section.

8.2.1 Ways to introduce non-linearity

There are three models to introduce non-linearity in the system.

- Non-linear feedback model.
- Non-linear combiner model.
- Non-linear filter generator model.

1. Non-linear feedback :- We make the feedback a non-linear Boolean function.
2. Non-linear combiner :- In the following diagram $f : \{0,1\}^m \to \{0,1\}$ is a non-linear combining function.

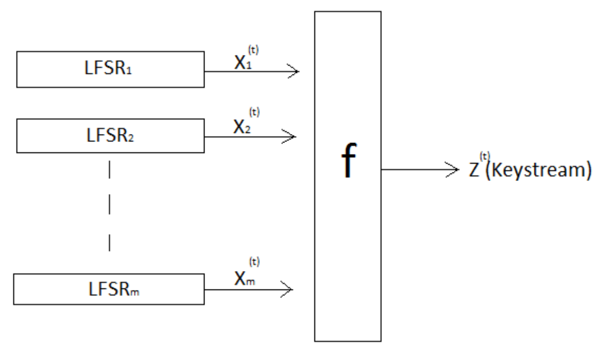

Figure 8.2: Non-linear combiner function

3. Non-linear filter generator :- This is described in the following figure. As before $f : \{0,1\}^m \to \{0,1\}$ is a non-linear Boolean function.

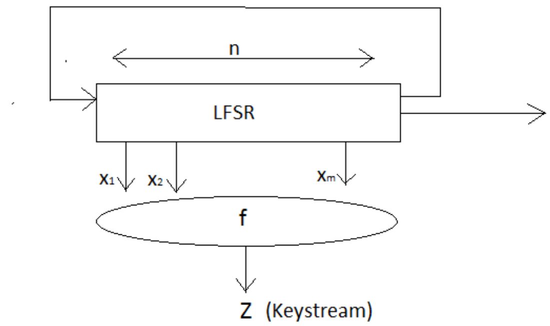

Figure 8.3: Non-linear combiner function

8.3 Nonlinearity

Definition 8.9 *A Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is called* <u>*linear*</u> *iff $\exists a_1, a_2, ..., a_n \in \{0,1\}$ such that $f(x_1, x_2, ..., x_n) = a_1x_1 \oplus a_2x_2 \oplus .. \oplus a_nx_n$.*

Definition 8.10 *A Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is called* <u>*affine*</u> *iff $\exists a_0, a_1, ..., a_n \in \{0,1\}$ such that $f(x_1, x_2, ..., x_n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus .. \oplus a_nx_n$.*

So if $a_0 = 1$, then f is the complement of a Boolean function.

Definition 8.11 *A Boolean function is said to be* <u>*non-linear*</u> *if it is not affine.*

The total number of n-variable Boolean functions is 2^{2^n}. From the above definition, the number of affine functions is 2^{n+1}. Hence the number of non-linear Boolean functions is $2^{2^n} - 2^{n+1}$.

Definition 8.12 *The distance between two n-variable Boolean functions f_1 and f_2, denoted by $d(f_1, f_2)$, is defined as the number of the Boolean vectors $\vec{x}$ such that $f_1(\vec{x}) \neq f_2(\vec{x})$.Equivalently it is defined as the number of 1's in $f_1 \oplus f_2$.*

Clearly d as defined above is a metric.

- Let $\mathcal{A}_n$ denote the set of all n-variable affine Boolean functions.

Definition 8.13 *The* <u>*non-linearity*</u> *of an n-variable Boolean function f is defined as*

$$nl(f) := \min_{g \in \mathcal{A}_n} d(f, g)$$

8.4 Cryptographic properties of Boolean functions

Some of the cryptographic properties of Boolean functions are listed below.

- Non-linearity
- Balancedness
- Correlation Immunity
- Algebraic Immunity
- ... etc. ...