Cryptography And Cryptanalysis

Ph. D. Course/ 2019-2020

Introduced By

Dr. Faez Hassan Ali

Lecture Four-1

Basic Efficiency Criteria of LFSR's-Systems

Introduction

As known before, any stream cipher key generator consists of two basic units; they are **sequence(s)** of bit stream generated from n-LFSR's and **Combining Function (CF)** for the key generator. Any weakness in any one of these units means clear weakness in output key generator sequence, so there are some conditions must be available in key generator before it is constructed.

In this lecture, we will introduce the **basic efficiency criteria** to estimate the sequence efficiency in order to use the sequence as encryption key. Every criterion will be discussed in details and introduce the basic conditions to obtain efficient KG.

The studies on the key generator sequence are applied to determine the sequence efficiency, so when be said "**efficient sequence**" that mean "**efficient key generator**" and vice versa.

Basic Efficiency Concept

The **basic efficiency** for KG can be defined as the ability of KG and its sequence to withstand the mathematical analytic which the cryptanalyst applied on them, this ability measured by some basic criteria to test KG efficiency (KGE).

The basic efficiency criteria (BEC) are used to determine the KGE, every BEC depend on some/all elements of LFSR and CF units, for this reason these criteria may be intersect each other's. If one criterion increased may cause negative effect on the others, which may be increase or decrease the ability of KGE. For instance, it's not necessary that the LC of KG be high as possible to gain efficient KG but it's very important that the efficient KG has balance CF to produce PRS.

It's important to mention that the zero input sequences must be avoided, this done when the all non-zeros initial values for LFSR's are chosen. The 1st condition to construct efficient KG is **"Choosing all non-zero's initial values for combined LFSR's"**, suppose that this condition is hold from now.

Let KG consist of n LFSR's have lengths $r_1,r_2,..,r_n$ respectively with $CF=F_n(x_1,x_2,\ldots,x_n)$, s.t. $x_i \in \{0,1\}$ $1 \le i \le n$, represents the output of $LFSR_i$, let $S=\{s_0,s_1,\ldots\}$ be the sequence product from KG and s_j, j=0,1,… represents elements of S. let S_i be the sequence i product from $LFSR_i$ with a_{ij} elements $1 \le i \le n$, j=0,1,…,. Lets denotes the KG which consists of n LFSR's by n-KG, so the linear system will be n-LKG, Product system will be n-PKG and Brüer will chosen to be 3-BKG.

Periodicity Criterion

The sequence S has period P(S) when $s_0=s_{P(S)}$, $s_1=s_{P(S)+1}$,…, the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers.

$P(S) = lcm(P(S_1),P(S_2),\ldots,P(S_k))$

if $P(S_i)$ are relatively prime to each other $\forall i$, $1\leq i\leq k$, then:

$$P(S)=\prod_{i=1}^{k} P(S_i)$$

Definition (3.1): Let $GCD_2=gcd(\prod_{i=1}^{1} m_i, m_2.GCD_1)=gcd(m_1,m_2)$, for convenient let $GCD_1=1$ and so on the general form of the recursion equation will be:

$$GCD_n=gcd(\prod_{i=1}^{n-1} m_i, m_n.GCD_{n-1}) \quad \ldots(3.3)$$

where $n\geq 2$ s.t m_i are positive integers, $\forall 1\leq i\leq n$.

Periodicity Criterion

Theorem (3.1): Let $m_i \in Z^+$, $\forall 1 \le i \le n$ then:

$$\mathrm{lcm}(m_1,m_2,\ldots,m_n)=\frac{\prod_{i=1}^{n} m_i}{\mathrm{GCD}_n(m_i)} \qquad \ldots(3.4)$$

(H.W.)

Example (1): Let $m_1=4$, $m_2=10$ and $m_3=15$, then:

L.H. of equation (3.4), lcm(4,10,15)=60.

R.H. of equation (3.4):

(4*10*15)/GCD(4,10,15)=600/gcd(4*10,15*gcd(4,10))=600/gcd(40,30)= 600/10=60.

From theorem (3.1), we obtain:

$$P(S)=\frac{\prod_{i=1}^{n} P(S_i)}{\mathrm{GCD}_n(P(S_i))} \qquad \ldots(3.7)$$

$$\text{s.t. } \mathrm{GCD}_n(P(S_i))=\gcd\left[\prod_{i=1}^{n-1} P(S_i), P(S_n)\cdot \mathrm{GCD}_{n-1}(P(S_i))\right]$$

The period of S which product from KG depends on the LFSR unit only and there is no effect of CF unit. P(S) will has lower bound when $r=r_i$ $\forall 1 \le i \le n$, and upper bound when $P(S_i)$ are relatively prime with each other $\forall i$, then $\mathrm{GCD}_n(P(S_i))=1$, therefore:

$$P(S_r) \le P(S) \le \prod_{i=1}^{n} P(S_i)$$

Periodicity Criterion

The condition to construct efficient KG is "**The periods (and automatically lengths) of combined LFSR's must be relatively prime**". It's known earlier that $P(S_i) \leq 2^{r_i} - 1$, and if the $LFSR_i$ has maximum period then $P(S_i) = 2^{r_i} - 1$, to gain maximum P(S), so if the 2nd condition has been satisfied, then $P(S) = \prod_{i=1}^{n} (2^{r_i} - 1)$, so the other condition is "**Each of the combined LFSR's in KG must have maximum period**". Let's suppose that the 2nd and 3rd conditions are holding from know.

Example (3.2):

Table (1) shows some examples of periods of KG's.

Table (1) Periods of different examples of KG's.

n	r_i	$P(S_i)$	P(S)
3	2,3,5	3, 7, 31	651
3	4,5,7	15, 31, 127	59055
4	2,3,5,7	3, 7, 31, 127	82677