Lecture Four

Basic Efficiency Criteria of LFSR's-Systems

1. Introduction

As known before, any stream cipher key generator consists of two basic units; they are sequence(s) of bit stream and **C**ombining **F**unction (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.

2. Basic Efficiency Concept

The **basic efficiency** for key generator can be defined as the ability of key generator and its sequence to withstand the mathematical analytic which the cryptanalyst applied on them, this ability measured by some basic criterions to test key generator efficiency.

The basic efficiency criterions are used to determine the KG efficiency, every criterion of efficiency depend on some/all elements of LFSR (Length and connection function) and CF (non-zero Inputs sequences and Output sequence) units, for this reason these criterions 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 KG efficiency. For instance, it's not necessary that the LC of key generator be high as possible to gain efficient KG but it's very important that the efficient key generator has balance CF (balance output bits and balance different strings in the produced sequence) to produce Pseudo Random Sequence (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 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. $x_i\in\{0,1\}$ $1\leq i\leq n$, represents the output of $LFSR_i$, let $S=\{s_0,s_1,\ldots\}$ be the sequence product from KG and s_j, $j=0,1,\ldots$ represents elements of S. let S_i be the sequence i product from $LFSR_i$ with a_{ij} elements $1\leq i\leq n$, $j=0,1,\ldots,$. Lets denotes the key generator 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.