Linear Complexity and Related Quality Measures for Cryptographic Sequences

Arne Winterhof[1] <arne.winterhof@oeaw.ac.at>

Let (s_n) be a sequence over the finite field F_p of prime order p. The *linear complexity* $L(s_n)$ of (s_n) over F_p is the length L of the shortest linear recurrence relation over F_p

$$s_{n+L} = c_{L-1}s_{n+L-1} + \ldots + c_0 s_n, \quad n \geq 0,$$

satisfied by (s_n). The linear complexity is a valuable measure for unpredictability and thus suitability for cryptography. It can be determined with the well known Berlekamp-Massey algorithm which is efficient for sequences with low linear complexity.
We discuss linear complexity and related measures as the *k-error linear complexity*, *linear complexity over different moduli* and the *correlation measure*. The connections between these quality measures are illustrated by results on the *Legendre sequence* (l_n) defined by

$$l_n = \begin{cases} \left(1 - \left(\frac{n}{p}\right)\right)/2 & \text{if } n \not\equiv 0 \bmod p, \\ 0 & \text{otherwise,} \end{cases} \qquad n \geq 0,$$

where $\left(\frac{n}{p}\right)$ denotes the *Legendre symbol*.

[1] H. Aly, A. Winterhof: *On the k-error linear complexity of Legendre and Sidelnikov sequences*, Preprint 2005.
[2] I. Shparlinski, A. Winterhof: *On the linear complexity of bounded integer sequences over different moduli*, Information Processing Letters, to appear.

[1]RICAM Austrian Academy of Sciences