On the Equivalence Classes of Certain Stream Ciphers

L. J. Garcia-Villalba and M. C. Rodriguez-Palanquex
Universidad Complutense de Madrid (U.C.M.), Spain

May 29, 2000

Most common sequence generators in stream cipher systems are based on a combination of one LFSR and a nonlinear function applied to the stages of the LFSR. In these cases the linear complexity is a measure of the suitability of a keystream for its cryptographic application. This parameter depends exclusively on the particular form of the filter and the LFSR minimal polynomial. Generally speaking, there is no systematic method to predict the resulting linear complexity. The present work is concerned with the problem of the determination of the number of nonlinear filters with different linear complexity.

It is known [2] that a filter F and their shifted versions, that is, the next family of filters .Also it is known [1] that a filter F and the family of 2^j-distant functions associated with this F have exactly the same period and linear complexity.

If we consider in the set of the nonlinear filters of order k with $k < L$ and L prime (which is the most common case), a class that contains the shifted filters of a certain filter f and its 2^j-distant filters, the number of possible classes, that is to say, the number of possible nonlinear filters with different cryptographic properties (of period and linear complexity) can be derived and is

$$N = \frac{\left(\begin{array}{c} 2^L - 2 \\ k - 1 \end{array} \right)}{L \cdot k}$$

References

[1] L. J. Garcia-Villalba *et al*, '2^j-Distant Nonlinear Filters: Pseudorandom Sequence Generators with Identical Cryptographic Properties'. Rump Session of Eurocrypt'99.

[2] R.A. Rueppel, 'Analysis and Design of Stream Ciphers'. Springer-Verlag, New York, 1986.