A NOTE ON SELF SHRINKING LAGGED FIBONACCI GENERATOR

Moon Kumar Chetry and W.B.Vasantha Kandasamy

Lagged Fibonacci Generator (LFG) are used as a building block of key stream generator in stream cipher cryptography. In this note, we have used the self shrinking concept in LFG and given an upper bound \( \frac{2^{nm}}{8} \) for the self shrinking LFG, where \( n \) is the number of stage and \( m \) is word size of the LFG.

We have also shown that the bound is attained by all the LFGs if degree \( n < 28 \), result supported by experiments.