INTERNATIONAL JOURNAL OF NETWORK SECURITY
Vol. 11
2010
58-60

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 $(2^{n+m}) / 8$ for the self shirking 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.

e-mail: vasanthakandasamy@gmail.com
web: http://mat.iitm.ac.in/wbv/public_html/home.htm