

A Short List of References on Pseudorandom Sequence/Number Generators

References

- [1] E.L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans. on Inform. Theory* vol. IT-22, No. 6, November 1976, pp. 732-736.
- [2] T. Herlestam, On Functions of Linear Shift Register Sequences, *Advances in Cryptology - Eurocrypt 1985 (Ed: Franz Pichler)*, Springer Lecture Notes in Computer Science, LNCS, vol. 0219, pp. 119-129, 1985.
- [3] R. A. Rueppel and O. J. Staffelbach, Products of linear recurring sequences with maximum complexity, *IEEE Trans. Inform. Theory*, vol. IT-33, No.1, Jan 1987, pp. 124 - 131.
- [4] T. Beth and F.Piper, The stop-and-go generator, *Advances in Cryptology, Eurocrypt'94*, vol. 209, Springer-Verlag, 1985, pp. 88-92.
- [5] Dieter Gollman and W.G. Chambers, Clock-controlled shift registers: a review, *IEEE Journal on Selected Areas in Communications*, vol. 7, No. 4, May 1989, pp.525-533.
- [6] C.G. Gunther, Alternating step generators controlled by de Bruijn sequences, *Advances in Cryptology, Eurocrypt'88*, Lecture Notes in Computer Science, vol. 304, Springer-Verlag, 1988, pp. 88-92.
- [7] D. Coppersmith, H. Krawczys and Y. Mansour, The shrinking generator, *Advances in Cryptology-Crypt'93*, Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 22-39.
- [8] W. Meier and O. Staffelbach, The self-shrinking generator, *Advances in Cryptology, Eurocrypt'94*, Lecture Notes in Computer Science, Springer-Verlag, 1994, pp. 205-214.
- [9] R.A. Rueppel, Stream ciphers, Chapter in *Contemporary Cryptology: The Science of Information Integrity*, G. J. Simmons, Ed. IEEE Press, New York, 1991, pp.65-134.
- [10] . Blum, M. Blum, and M. Shub, A Simple Unpredictable Pseudo-Random Number Generator, *SIAM J. Comput.* , vol.15, No. 2, 1986. pp.364-383.
- [11] . W. Cusick, Properties of the $x^2 \bmod N$ pseudorandom number generator, *IEEE Trans. on Inform. Theory* vol. IT-41, No. 4, July 1995, pp. 1155-1159.