MATHEMATICA, Tome 51(74), N° 2, 2009, pp. 163–171

COMBINING THE SOLITAIRE ENCRYPTION ALGORITHM WITH LAGGED FIBONACCI PSEUDORANDOM NUMBER GENERATORS

CHRISTIAN SĂCĂREA, CSABA SZÁNTÓ and ISTVÁN ŞUTEU SZÖLLŐSI

Abstract. We use a "byte" variant of Bruce Schneier's Solitaire Encryption Algorithm to produce the seed and weight system of a lagged Fibonacci pseudorandom number generator which generates a sequence of bytes. We analyze variants of the procedure above by testing them using some up to date randomness tests.

MSC 2000. 65C10.

Key words. Pseudorandom number generator, lagged Fibonacci generator, Solitaire algorithm.

REFERENCES

[1] Janke, W., *Pseudo Random Numbers: Generation and Quality Checks*, Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms, Lecture Notes, J. Grotendorst, D. Marx, A. Muramatsu (Eds.), John von Neumann Institute for Computing, NIC Series, Vol. **10**, 447–458.

[2] `http://en.wikipedia.org/wiki/Pseudorandom_number_generator`

[3] `http://csrc.nist.gov/groups/ST/toolkit/rng/stats_tests.html`

[4] `http://www.schneier.com/solitaire.html`

[5] `http://www.lavarnd.org/what/nist-test.html`

Received December 1, 2008
Accepted March 11, 2009

"Babeş-Bolyai" University Cluj
Faculty of Mathematics and Computer Science
Str. M. Kogălniceanu nr.1.
RO-400084 Cluj-Napoca, România
E-mail: `csacarea@math.ubbcluj.ro`
E-mail: `szanto.cs@gmail.com`

The research for this paper was supported by grant PN2-P4-11-020/2007.