Clock-Controlled Shrinking Generator Of Feedback Shift Registers

Kanso, A

SPRINGER-VERLAG BERLIN, INFORMATION SECURITY AND PRIVACY, PROCEEDINGS; pp: 443-451; Vol: 2727

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

A system related to the shrinking generator that is made up of two feedback shift registers in which one (FSR A) controls the clocking of the other (FSR B) is introduced. It is established that if FSR A generates an m-sequence of period (2(m)-1) and FSR B generates a de Bruijn sequence of period 2(eta), then the output sequence of the system has period P = 2(m+eta-1), linear complexityL bounded from below by 2(m+eta-2) good statistical properties, and it is secure against correlation attacks. All these properties make it a suitable crypto-generator for stream cipher applications.

References:

1. CHAMBERS WG, 1984, ELECTRON LETT, V20, P1018
2. COOPERSMITH D, 1994, P CRYPT 93, P22
3. GOLIC JD, 1991, J CRYPTOL, V3, P201
4. GOLIC JD, 1994, LECT NOTES COMPUTER, V809, P90
5. GOLIC JD, 1995, LECT NOTES COMPUTER, V921, P248
6. GOLIC JD, 1995, LECT NOTES COMPUTER, V950, P230
7. GOLLMANN D, 1989, IEEE J SEL AREA COMM, V7, P525
8. GOLOMB SW, 1982, SHIFT REGISTER SEQUE
9. JOHANSSON T, 1998, LECT NOTES COMPUT SC, V1514, P342
10. JOHANSSON T, 1999, LECT NOTES COMPUT SC, V1592, P347
11. JOHANSSON T, 2000, LECT NOTES COMPUT SC, V1880, P300
12. KANSO A, 1999, THESIS U LONDON, P161
13. LIDL R, 1986, INTRO FINITE FIELDS
14. MEIR W, 1989, J CRYPTOL, V1, P159
15. MIHALJEVIC M, 1993, LECT NOTES COMPUTER, V178, P349
16. SIEGENTHALER T, 1984, IEEE T INFORM THEORY, V30, P776
17. SIMPSON L, ACISP 1998, P147

For pre-prints please write to: abstracts@kfupm.edu.sa