Pseudo Random Number Generation on FPGA

Tamás Herendi[*,**]

[*] University of Debrecen/Faculty of Informatics, Debrecen, Hungary

Abstract—**The aim of the present paper is to show the theoretical background of the construction of uniformly distributed (UD) pseudo random number (PRN) sequences with good properties and efficient implementation on FPGA.**

REFERENCES

[1] T. Herendi "Uniform distribution of linear recurring sequences modulo prime powers", *Journal of Finite Fields and Applications*, vol.10, 2004, pp. 1–23

[2] T. Herendi "Construction of uniformly distributed linear recurring sequences modulo powers of 2", in press

[3] T. Herendi and S.R. Major "Modular exponentiation of matrices on FPGA-s", in press

[4] D.E. Knuth, *The art of computer programming*, Addison-Wesley,1973

[5] R. Lidl, H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986

[6] H. Niederreiter, J.S.Shiue "Equidistribution of linear recurring sequences in finite fields", *Indag. Math.*, vol. 39, 1977 pp. 397--405

[7] H. Niederreiter, J.S.Shiue "Equidistribution of linear recurring sequences in finite fields II", *Acta Arith*., vol. 38, 1980, pp. 197—207