CORR 99-54

Non-Linear Complexity of the Naor-Reingold Pseudo-Random Function

William D. Banks*, Frances Griffin*, Daniel Lieman*, Igor E. Shparlinshi*

Abstract We obtain an exponential lower bound on the non-linear complexity of the new pseudo-random function introduced recently by M. Naor and O. Reingold. This bound extends and generalizes the lower bound on the linear complexity of this function that has recently been obtained by F. Griffin and I.E. Shparlinshi.