1072-94-203 **Kenneth R. Matheis**, **Rainer Steinwandt*** (rsteinwa@fau.edu) and **Adriana Suárez Corona**. *Algebraic properties of a lightweight block cipher.*

The block cipher DESL is a *DES Lightweight extension* which has been proposed at FSE 2007 by Leander et al. The structure of this block cipher is basically identical to DES, but differing from the latter, in DESL all S-boxes are identical. This talk discusses the permutation group generated by the round functions of DESL and reports on experiments with an algebraic attack known as *Multiple Right Hand Sides* when being applied to full and reduced round versions of DESL. (Received June 28, 2011)