A characterization of regular mappings

Horacio Tapia
UAM–Iztapalapa

(joint work with G. Vega)

Substitution boxes (S–boxes) are one of the main components in DES type ciphering systems. Since the appearence of differential and linear cryptanalysis the development and design of substitution boxes which can be immune against these types of cryptanalysis has become an active research topic. In this talk a characterization of regular mappings is given in terms of the corresponding difference distribution table. Also an equivalence relation on the set of regular mappings is defined in such a way that each equivalence class has the same difference distribution table.

Key words: substitution boxes (S–boxes), block ciphers, regular mappings, difference distribution tables.